MODELING INFORMATION ASSURANCE

THESIS

Joseph Edward Beauregard, 2nd Lieutenant, USAF

AFIT/GOR/ENS/01M-03

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U. S. Government.

AFIT/GOR/ENS/01M-03

MODELING INFORMATION ASSURANCE

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Joseph E. Beauregard, B. S.

2nd Lieutenant, USAF

March 2001

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GOR/ENS/01M-03

MODELING INFORMATION ASSURANCE

Joseph E. Beauregard
2nd Lieutenant, USAF

Approved:

05 March 01

Richard F. Deckro, DBA (Advisor)
Professor of Operations Research
Department of Operational Sciences

Date

05 MAR 01

Stephen P. Chambal, PhD, Captain, USAF (Reader)
Assistant Professor of Operations Research
Department of Operational Sciences

Date

ACKNOWLEDGEMENTS

This thesis could not have been possible without the help of several dedicated people. I would first like to give thanks to my Advisor, Dr. Richard Deckro, who is truly devoted to his students and their success. His patience with a young 2nd Lieutenant is not to be underestimated, nor tested.

A special thanks is also given to my Reader, Captain Stephen Chambal. His knowledge in Operations Research, specifically in the area of Value Focused Thinking, has certainly provided this thesis effort both guidance and expertise.

Finally, I would like to express my sincere appreciation to the extraordinary personnel at the Air Force Technical Applications Center located at Patrick Air Force Base, Florida. This thesis would not have been possible without their willingness to go above and beyond their already demanding schedule to make this project a truly enjoyable and rewarding experience.

Joe Beauregard

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

LIST OF EQUATIONS

AFIT/GOR/ENS/01M-03

ABSTRACT

The ever-increasing speed of information systems allows decision-makers around the world to gather, process, and disseminate information almost instantaneously. However, with this benefit there comes a price. Information is valuable and therefore a target to those who do not have it or wish to destroy it. The Internet has allowed information to flow freely, but it has also made information vulnerable to many forms of corruption. The U. S. military controls much of the world's most sensitive information, and since it cannot sacrifice losing the speed at which this information is currently processed and disseminated, it must find a way to assure its protection. There has been some effort to model information assurance in recent years, however the no accepted quantifiable model currently exists.

This study presents a strategy to aid organizations, specifically organizations within the Department of Defense (DoD), in their efforts to protect valuable information and information systems. The model is reviewed and results from an actual analysis are presented.

MODELING INFORMATION ASSURANCE

1. Introduction

1.1 Background

Like many great technological advances, the unprecedented growth of the Internet has spawned new businesses, opportunities, ideas, and unfortunately, new problems. The Internet created a global community that knows no geographic boundaries; the ability to send and receive information freely and instantaneously has radically and permanently changed the speed at which the world operates. Decision-makers can now gather, process, and distribute information virtually instantaneously. This decision making process is used worldwide in endeavors ranging from small family businesses to national governments and transnational organizations. However, this free flow of information across communication networks also produces a major vulnerability inherent to the Internet. No nation or group is more exposed than the United States and its military. Although the U. S. Department of Defense (DoD) was responsible for creating the predecessor to today's Internet, it was not originally designed to transfer information critical to U. S. national security, nor was it built for access by untrustworthy users. This thesis proposes a strategy to aid organizations, specifically organizations within the Department of Defense, in their efforts to protect valuable information and information systems.

The beginnings of the Internet trace back to the late 1950's when then President Dwight D. Eisenhower formed the Advanced Research Projects Agency (ARPA) in response to the Soviet satellite launching of Sputnik [Gromov, 2000]. In 1962, ARPA researcher Dr. J. C. R. Licklider was chosen to head the Information Processing Techniques Office, a division focused solely on developing and improving the military's computer technology [Zakon, 2000]. Work soon began on ARPANET, a computer network designed to facilitate communication between several universities involved in the project. ARPANET was finally operational in September of 1969 when researchers of the University of California Los Angeles (UCLA) successfully, although briefly, logged into Stanford Research Institute (SRI) computers [Gromov, 2000].

ARPANET and other computer communication networks like it continued to evolve throughout the 1970's and early 1980's. In 1982, DARPA, (formerly ARPA, renamed the Defense Advanced Research Projects Agency in 1972) in cooperation with the Defense Communications Agency (DCA, now the Defense Information Systems Agency, DISA), established the first Transmission Control Protocol / Internet Protocol (TCP / IP) connection. This event is officially recognized as the beginning of the Internet as it is known today [Zakon, 2000].

Security problems began almost immediately after the creation of the Internet. Within two years, the Internet was experiencing 1,000 host breaks a year; by 1987 this number had grown to 10,000 [Zakon, 2000]. The Internet, built from ARPANET's policy of openness and flexibility, was simply not designed for the security necessary to perform commercial and governmental demands [Longstaff, Ellis, Hernan, Lipson, McMillan, Pesante, and Simmel, 1997]. A new vulnerability in the United States and its military had been exposed.

The U. S. military must make rapid, informed decisions in order to remain the strongest force in the world. Networked computer systems that can gather, process, and disseminate information quickly in order to "serve the Department of Defense's local, national, and worldwide information needs" are necessary to accomplish this task [AFDD 2-5, 1998: 4]. Interrupting, destroying, or otherwise corrupting this information causes the decision making process to slow, which in turn reduces the ability of the military to defend the country and creates an opportunity for valuable information to be corrupted, lost, or stolen. The advent of computers and the Internet has created a new type of warfare where information, information systems, and information processes, rather than weapons or structures, are the targets. The results of a successful attack on a sensitive government system could be devastating to national security.

Air Force Doctrine Document (AFDD) *1: Air Force Basic Doctrine* (September, 1997), the fundamental doctrine document for the U. S. Air Force, states that

> Warfare is normally associated with the different mediums of land, sea, air, and space. *In addition, information is now considered another medium in which some aspects of warfare can be conducted* [AFDD 1, 1991: 7].

The United States is more vulnerable to an information attack than any other nation due to an array of political and military factors. The U. S. is the only true superpower that exists today, making it a natural target for countries that wish to overtake that role or who simply want to do harm. However, few countries, if any, will realistically want to face the United States in a classic war. A well-planned information attack against the U. S.

may mitigate some of the nation's battlefield advantage, if even temporarily, making the United States vulnerable to other conventional and unconventional attacks. The asymmetric nature of an information attack, coupled with its stealth capabilities, make it an ideal weapon for a nation state, national group, or transnational organization to use against a military superpower.

Unlike a traditional attack, a potentially crippling information attack can come from anyone at any time. If executed correctly, a single person could launch an information attack powerful enough to severely cripple many sectors of the American infrastructure. A small team of people could do even more damage in a shorter amount of time. Often an attack may not even be detected until it is well in progress or completed; this makes even determining who is attacking quite difficult. Information itself can also be a target; classified material concerning U. S. war plans, technology, and even personnel can provide the enemy with critical information that could compromise national safety.

No system in operational use will ever be completely safe from attack; however, the more that is known about an organization's system vulnerabilities, the better prepared that organization will be should an attack come. If system vulnerabilities can be identified before an enemy is able to exploit them, then the necessary steps to mitigate these problems can be taken. The goal of this study is, therefore, to develop a model to measure the level of information assurance (IA) for a DoD organization's information system. Joint Doctrine defines information assurance as:

> Information Operations (IO) that protect and defend information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information

> systems by incorporating protection, detection, and reaction capabilities [JP 3-13, 1998: I-9].

The difficulty in increasing IA lies in the balance between the level of IA and its impact on system operational capability and resource costs [Hamill, 2000: 4-1]. Whenever system IA is increased, the operational capability for that system is potentially impacted. Increasing IA to a maximum attainable level, which would secure the system but render it operationally useless, would be no better (and perhaps worse) than not securing it all. The solution to assuring a system is finding a balance between the level of IA and its impact on system operational capability that falls somewhere between the extremes of making a system so secure that it becomes ineffective, or so insecure that it becomes an easy target. Since different systems contain different information, where the balance point falls between these extremes will depend on the system itself.

In addition to impacting system operational capability, every IA strategy consumes a certain amount of the organization's resources. A resource cost is defined to be any cost associated with implementing an IA strategy, whether it is a fiscal cost or a personnel cost. An information assurance strategy that greatly improves IA and system operational capability that is too expensive will not be implemented, and is consequently not helpful to the organization. Therefore, in order to obtain a true IA measure, the level of IA gained by a strategy, the potential impact the strategy will have on system operational capability, and cost of such an implementation must all be considered.

1.2 Problem Statement

Every military and civilian organization is susceptible to information attacks in a variety of forms. It is therefore necessary to develop a methodology for measuring how assured an organization is against an information compromise, and to provide that organization with insight as to how they can improve their level of assurance. However, resource costs and system operational capability may be impacted whenever an assurance strategy is implemented and therefore must also be considered in the model.

This thesis utilized three separate hierarchical models that measure the total level of information assurance as a tradeoff between IA, the change in system operational capability incurred by the IA strategy, and the resource cost of implementing the strategy. The models and their associated measures then aid in identifying what information assurance strategies, if any, would be most beneficial.

1.3 Information System under Study

Several Air Force organizations were contacted regarding participation in this study. After reviewing a range of systems, the kind offer of the Air Force Technical Applications Center (AFTAC) was accepted. AFTAC, located at Patrick AFB, FL, agreed to undertake this 'challenge' and volunteered their AFTAC Mission Information System (AMIS) to be studied. The sole criterion for selecting a system was that it contain valuable information the organization needed to protect. AMIS satisfied this condition as it is classified a SECRET system. AFTAC personnel served as the system's experts to help create value hierarchies, single dimensional measure functions, and score their system and a set of possible IA options. Their willingness to take on this extra duty is greatly appreciated. This project could not have been completed without their dedicated efforts.

1.4 Importance of Project

The number of computer security incidents has been steadily increasing over the past decade. As the Internet grows, so does the likelihood of an unauthorized system penetration. In December 1988, DARPA (the same organization responsible for building the ARPANET and then the Internet, detailed above) formed the Computer Emergency Response Team (CERT) in reaction to an Internet virus known as the "Morris Worm," which brought down nearly 10% of the entire Internet at the time [CERT/CC, 2000]. Since 1988, the team has evolved into the CERT Coordination Center and is responsible for reporting major security incidents over the Internet. Figure 1-1, taken from data on the CERT Web site, shows the number of incidents *identified* and subsequently *reported* to CERT since 1988:

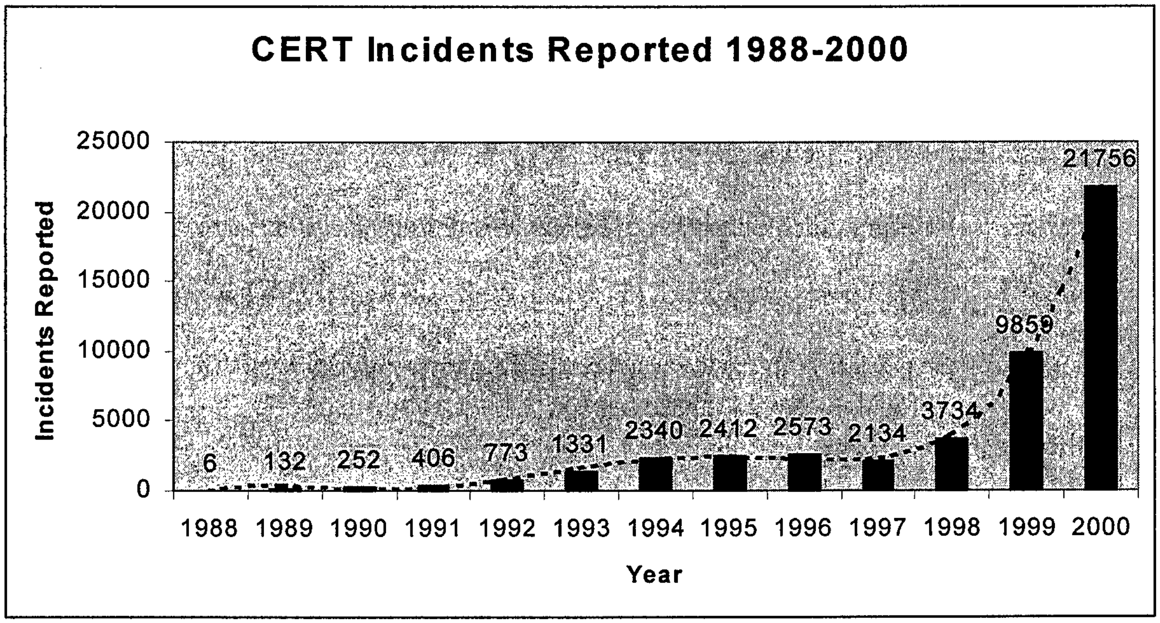


Figure 1-1: CERT Statistics on Incidents per Year [CERT/CC, 2001].

This chart represents only the incidents actually reported to CERT, which suggests that there may be thousands more incidents that go either undetected or unreported. Any one of the thousands of incidents portrayed above has the potential to do severe damage to the U. S. military, U. S. national infrastructure, or private business. Notice that of the 47,708 total incidents reported to CERT from 1988-2000, 21,756 (approximately 45.6%) occurred in year 2000 alone. If the number of incidents continues to rise at this rate, a disaster is inevitable. Information assurance is the first step in preventing such a disaster.

The Air Force Computer Emergency Response Team (AFCERT), established in 1992, is the AF equivalent to CERT. The mission of AFCERT is to "conduct operations involving intrusion detection, incident response, computer security information assistance, and vulnerability assessment of Air Force automated information systems" [AFCERT, 2001]. AFCERT also records information detailing the number of system incidents reported by Air Force organizations. Figure 1-2 is an inverted pyramid chart showing incident classifications for the year 1999:

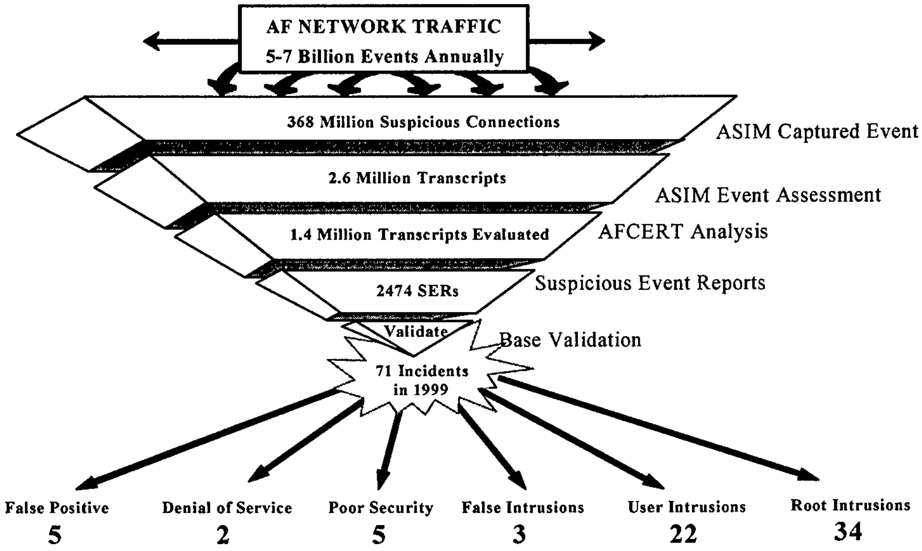


Figure 1-2: 1999 AFCERT Analysis

Approximately 368 million events out of some 5 to 7 billion events were classified as suspicious connections. Each of these suspicious connections had to be analyzed, and further action was taken on those that necessitated it. Buried in the 368 million suspicious connections were 71 incidents that AFCERT determined to be of malicious intent to the Air Force. While five of these incidents proved to be false positives, any one of the remaining 66 incidents had the potential to severely damage U. S. national security.

Currently there are very few available methods that would allow organizations to measure the level of IA in a given system. While all organizations strive to protect their resources as best they can, there is no universally accepted way to quantitatively determine exactly what level of assurance they have, nor what new IA technologies will best help them improve their assurance level. This thesis presents an organization with a specific model that provides valuable insight as to the best way to improve their information assurance and at what cost.

1.5 Research Approach

As previously mentioned, the problem has three objectives: measure and potentially increase the level of IA at AFTAC while accounting for the impact of the IA strategy on system operational capability and resource costs. Since each organization will value IA, resource costs, and system operational capability differently, one universal best-case solution for this problem may not be desirable. Depending on how organizations *value* each of the objectives, it is very possible that ten organizations can have ten different solutions, all equally valid for their specific mission objectives. The project is therefore tailored to AFTAC's AMIS system using an approach known as Value Focused Thinking (VFT). However, application of the basic model and methodology to other organizations and systems is possible and encouraged.

VFT focuses on the values of the decision-maker rather than a proposed set of alternatives. A value hierarchy is created to represent what the decision-maker feels is important to the project. A measure is developed to represent each value; these values are then weighted by the decision-maker based upon the range of the measure. It is this weighting process that allows a general model to be tailored to a specific commander or organization. Different alternatives, including the current state of the system, are then scored and ranked, producing a measure of best alternatives derived directly from the decision-maker's values.

1.6 Thesis Overview and Format

A literature review of military information assurance doctrine, computer security in the public sector, past attempts at modeling IA, and a review of VFT theory will follow in Chapter 2. A description of the methodology used to accomplish the research in this study and the creation of the value hierarchies will be detailed in Chapter 3. Chapter 4 presents the results of the analysis, including strategy rankings based on the decision-maker's value weights. A sensitivity analysis on the hierarchy weights is also presented in Chapter 4. Finally, Chapter 5 will be a discussion on the conclusions drawn from the study and potential opportunities for future work. The Appendix is a detailed summary of the values within the hierarchy and their associated measure functions developed in cooperation with AFTAC and the selected information system.

2. Literature Review

This chapter focuses on previous work in the field of Information Assurance (IA) and Value Focused Thinking (VFT). A review of Department of Defense (DoD) doctrine and civilian industry standards provides the scope needed to show the importance of IA in today's environment and to provide the foundation for the models developed. The doctrine review is followed by a detailed discussion of Value Focused Thinking, which will provide the framework used to attack the problem of modeling information assurance. Finally, past and present work on IA models will be presented in order to gain fundamental insight on modeling techniques that have been successful.

2.1 Department of Defense Doctrine

To effectively measure information assurance in military organizations it is essential that the elements of IA the DoD feels are important be correctly captured within the model. Therefore published DoD doctrine, which is the official position of the U. S. Government, was used as expert sources.

Information operations have become one of the most important issues in defense doctrine. *Air Force Doctrine Document 2-5: Information Operations* states that "dominating the information spectrum is as critical to conflict now as controlling air and space, or occupying land was in the past, and is viewed as an indispensable and synergistic component of aerospace power" [AFDD 2-5, 1998: 5].

While doctrine on IA does exist, it is still a relatively new and developing field. There are several ways IA is defined, however the definition given in Chapter 1 from

Joint Publication 3-13: Joint Doctrine for Information Operations will be the definition used throughout the study:

> Information assurance is defined as Information Operations (IO) that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities [JP 3-13, 1998: I-9].

The terms availability, integrity, authentication, confidentiality, and nonrepudiation are considered objectives of information assurance and are defined by *JP 3-13* in the context of IA in Table 2-1:

Table 2-1: Definitions of Information Assurance Objectives [JP 3-13 1998: III-3]

Definitions of IA Objectives	
Availability	Assured access by authorized users
Integrity	Protection from unauthorized change
Authentication	Verification of the originator
Confidentiality	Protection from unauthorized disclosure
Non-Repudiation	Undeniable proof of participation

Information Operations is a broad term defined by Joint Doctrine as follows:

> actions taken to affect adversary information and information systems while defending one's own information and information systems. IO apply across all phases of an operation, the range of military operations, and at every level of war [JP 3-13, 1998: I-1].

Information assurance therefore is a subcategory of information operations; specifically, IA covers the defensive realm of information operations. Figure 2-1, taken from *JP 3-13*, illustrates the role of information assurance in the information operations spectrum:

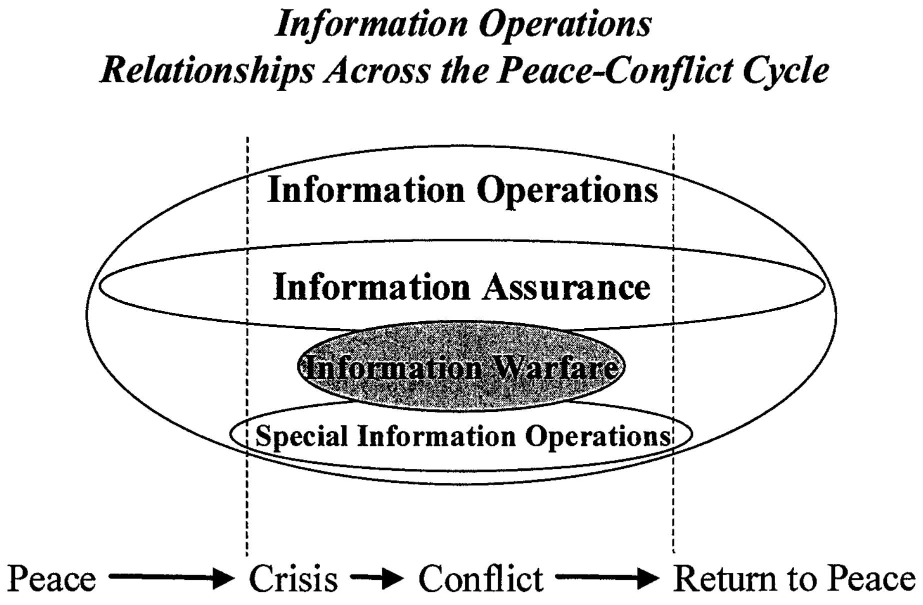


Figure 2-1: Information Operations Spectrum [JP 3-13, 1998: I-4]

Figure 2-1 shows IA as a continuous process; it covers the entire range of information operations from peacetime through a major conflict and back to peace. The U. S. cannot afford to focus on the importance of IA only when a conflict arises; it demands strict vigilance at all times. The U. S. is continuously vulnerable to an information attack and therefore must always protect against one. An IA model must capture all the elements of doctrine discussed above in a quantifiable manner so it can determine if the organization under study meets these requirements, and if they do not meet them, where they are most vulnerable. The model must also show the protection, detection, and reaction capabilities of the organization under study.

Information assurance is therefore the continual process of system management whereby:

1) Authorized users can access the system

2) Unauthorized users cannot access the system

3) Information is not lost, stolen, or corrupted

4) Users and transmissions can be monitored

5) Intrusions can be detected

6) Actions can be taken during and after an intrusion

The above list is not meant to be an all-inclusive representation of information assurance, but rather a starting point given by DoD doctrine that all organizations must adhere.

2.2 Protection, Detection, Reaction

Protection is the first line of defense in any system; if the enemy cannot penetrate the system then information cannot be compromised. However, in order to protect systems appropriately, detailed knowledge of the threats to the system must first be obtained. Acquiring such knowledge is no easy task in today's volatile social and political environment. A collection of potential threats that include terrorist groups, computer hackers, and foreign nations are all equally capable of launching an information attack. Speaking in terms of firepower alone, the United States military is perhaps the strongest force the world has ever seen, yet it is more vulnerable now then ever to an information operations attack. Information warfare is a potential "Achilles' heel' of the United States [which] can be the great equalizer for a militarily inferior adversary" [AFDD 2-5, 1998: 6].

The threat of an electronic attack against the United States is mainly due to the free flow of information allowed by the Internet. Since almost anyone can gain access to the Internet, the list of potential attackers is virtually limitless. Defending against all these threats requires what the DoD calls information superiority, defined as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same" [JP 3-13, 1998: I-10]. Air Force doctrine also provides an alternate definition for information superiority: "that degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition" [AFDD 2-5, 1998: 42]. Information superiority gives the U. S. the ability to control information even on an insecure network such as the Internet. Since information superiority cannot be obtained and maintained without information assurance, to control the information operations (IO) spectrum, the U. S. military must have the ability to protect its own information, detect any unauthorized intrusions, and react to those intrusions in a timely fashion.

Information assurance is contained under the Defensive Counterinformation (DCI) subcategory of the Information Superiority hierarchy, shown as Figure 2-2. The chart shows that defensive counterinformation and offensive counterinformation (OCI) are interrelated, indicating that offensive IO techniques must be used to gather information from enemies while at the same time defending friendly information from attack [AFDD 2-5, 1998: 3].

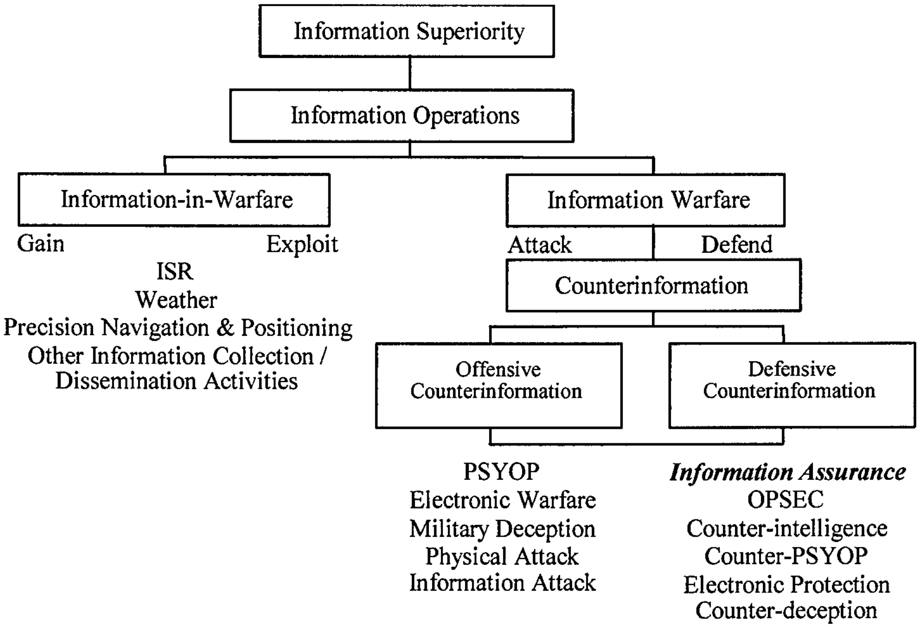


Figure 2-2: Air Force Information Superiority Construct [AFDD 2-5, 1998: 3]

Offensive counterinformation is defined to be:

> **Actions** taken to **control** the information environment. OCI operations are designed to *limit, degrade, disrupt, or destroy* adversary information capabilities and are dependent on having an understanding of an adversary's information capabilities [AFDD 2-5, 1998: 10].

Similarly, Air Force doctrine defines defensive counterinformation as:

> **Actions** that **protect** information, information systems, and information operations from any potential adversary. DCI includes such programs as *operations security (OPSEC), information assurance, and counterintelligence* [AFDD 2-5, 1998: 10].

Information superiority requires that both OCI and DCI be performed equally well in order to control the information environment; failure to do so will prevent the U. S. military from controlling the information operations spectrum.

2.3 INFOCON Levels

The threat of information warfare prompted the DoD to implement the Information Operations Condition (INFOCON) system. Chairman of the Joint Chiefs of Staff (CJCS) Memo CM-510-00 describes INFOCON as:

> A comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack and measures the focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems [CJCS Memorandum CM-510-00, 1999].

Table 2-2 outlines the INFOCON levels as reported by AFTAC:

Table 2-2: INFOCON Levels

INFOCON Level	Threat Assessment
INFOCON ALPHA	Indications and warnings of a general threat resulting from a possible regional event, system probe, or planned exercise
INFOCON BRAVO	Indications that specific system being targeted, detection of significant and concentrated network reconnaissance, or network penetration resulting in no impact on DoD operations.
INFOCON CHARLIE	Limited impact attacks detected or imminent, although attacks are successfully counteracted and missions are still able to be accomplished
INFOCON DELTA	General attack implying impact on DoD operations, loss in system functionality, and significant risk of mission failure [AFTAC, 2001].

U. S. military doctrine clearly shows the importance of IA and the role it will play in the emerging information era. The capability to physically attack the United States is limited; however the potential damage that can result from an information attack makes U. S. information, information systems, and information processes prime targets. It is easy to see that a compromise of sensitive U. S. information or data could lead to military disasters. Similarly, an attack on U. S. nationwide critical infrastructures could be of equal or greater consequence.

2.4 Critical Infrastructure Assurance

Computers and technology have become so integrated in society that their services are taken for granted. All key infrastructures in the United States are now automated to some degree, making life move faster and somewhat easier for everyone. However, the ability of technology to provide Americans with an easier life has also created a major vulnerability. An information failure on a critical infrastructure system, due to natural causes or malicious attack, could cripple the country. This criticality is so important that in July of 1996 then President Clinton signed Executive Order 13010 establishing the President's Commission on Critical Infrastructure Protection (PCCIP), which was tasked with "developing a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats" [Information Assurance 1999: ES2]. Specifically, the PCCIP was tasked to look at the five following infrastructure sectors:

1) Information and Communications
2) Banking and Finance
3) Energy, Including Electrical Power, Oil and Gas
4) Physical Distribution
5) Vital Human Services [PCCIP, 1997: 2].

Critical Infrastructures form the backbone of the country; they include such entities as highways, water supplies, electric companies, and financial institutions. They exist to support the citizens of the U. S. and their economy. These infrastructures bring citizens services they cannot provide for themselves. The PCCIP states:

> The development of the computer and its astonishingly rapid improvements have ushered in the Information Age that affects almost all aspects of American commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers [PCCIP, 1997: 3].

All infrastructures, military and civilian, are computer operated in one form or another and thus susceptible to an information attack.

In the 1997 exercise ELIGIBLE RECEIVER, a covert simulated attack on the nation's infrastructures ordered by the Joint Chiefs of Staff, proved that by using only open source intelligence and widely available hacker tools that U. S. infrastructures were quite vulnerable to malicious attack [Information Assurance 1999: ES3]. These finding were proven to be true in 1998 when a group of U. S. teenagers and an Israeli mentor were able to penetrate DoD logistics, finance, and personnel records in what came to be known as the SOLAR SUNRISE intrusions [Information Assurance, 1999: ES3]. If a group of U. S. teenagers were able to gain unauthorized access into these systems with relative ease, then certainly a highly trained hostile force could enter these systems and cause tremendous damage.

In response to ELIGIBLE RECEIVER and SOLAR SUNRISE, the White House released Presidential Decision Directive 63 in May of 1998 which:

1) Established a national goal for infrastructure protection

2) Created a national structure much like that recommended by the President's Commission

3) Provided guidelines on infrastructure protection

4) Required each Federal department and agency to assign IA responsibilities to the Chief Information Officer and appoint a Chief Infrastructure Assurance Officer

5) Called for a National Infrastructure Assurance Plan to address specific tasks such as vulnerability analyses, warning, response, reconstitution, etc. [Information Assurance, 1999: ES3].

A national plan similar to the DoD assurance objectives was called for to protect critical infrastructures. Presidential Directive 63 made information assurance a national concern, although it took a near disaster for this to occur. Private business also followed suit after realizing that they were also targets for cyber attack.

2.5 Private Sector IA Concerns

The Internet created a brand new business market and communication medium for people around the world to utilize. If a product exists, chances are it is available from the Internet through either a retailer or a private individual. "With information from many sources but a click away . . . this globe-spanning network's ability to let us check and compare prices for similar goods and services" generally offers the consumer a lower cost than the neighborhood store [Harrow, 1998].

The Internet allows consumers the ability to search for and purchase goods directly from their own home, making shopping more convenient and less expensive. However, there are risks associated with purchasing goods via the Internet; personal financial information, whether a valid credit card number, checking account, or other data, is required. A faulty security system, even on a trusted site, could lead to unauthorized persons fraudulently using stolen information to purchase on-line goods and services.

An experienced hacker or group of hackers could steal thousands of credit card numbers a day if they are able to bypass a site's security system. One group of eleven people, known as the "Phone Masters," accomplished such a feat by breaking into several local and long distance telephone companies, credit reporting firms, and even the FBI's Crime Information Center [Holzinger, 2000: 32]. The group stole consumer credit card information and sold it worldwide. An estimated $1.1 to $1.5 million dollars was lost due to "Phone Master" activities; FBI agent Michael Morris stated "They could have - temporarily at least - crippled the nation's phone network . . . What scares me the most is that [the Phone Masters gang] could have done a lot more damage" [Holzinger, 2000: 32].

In a recent survey by PricewaterhouseCoopers and *Information Week* magazine of 1,600 information security professionals in 50 countries, it was determined that on-line businesses were found to be the most at risk group for Internet attacks. The survey found that on-line businesses could expect three times the amount of attempted hacks to their system compared to non-commerce sites, and they could lose up to seven times more revenue due to these hacks [Holzinger, 2000: 33].

Many corporations, DoD organizations, and other interest groups use their World Wide Web sites not for business but to help expand their influence or provide information to users and subscribers. While these sites are not attacked for financial gain, they are often attacked simply to prove it can be done or to protest some social or political point of view. The chart from CERT, shown as Figure 1-1 in Chapter 1, illustrates the growing trend of malicious Internet attacks.

The widespread use of electronic mail (e-mail) has created another opportunity for malicious attack on computer systems. In May of 2000, the "I Love You" computer virus passed through an estimated 500,000 systems, crippling numerous sites by flooding their email and erasing countless multimedia files [CERT: *Advisory,* 2000].

Another barrier in the search for universal IA concerns the legal ramifications of the Internet. Currently, U. S. codes of law dictate that "concepts of jurisdiction are principally based on notions of physical presence within a jurisdiction" [Donohue, 1997: 7]. However, a crime can be committed via the Internet from almost any location in the world, which makes capturing and trying suspected Internet criminals very difficult.

There are three specific factors of the Internet that makes legal prosecution nearly impossible:

- **Location of Machines:** The Internet permits interaction between people who do not know each other's physical locations, therefore they cannot know the laws of the other's persons residence

- **Caching:** The process where information to servers is copied on the user's hard drive so that future trips to the same Web site will be less time consuming. While caching is essential to the speed of operation, it prevents the computer from distinguishing an original source from a cache.

- **Hyperlink:** Allows one Web site to connect to another, regardless of location. One Web site may be in a certain legal jurisdiction, while the other may not. A legal dilemma arises when the nonresident site posts illegal subject matter (however defined in that jurisdiction) through the resident site [Donohue, 1997: 7-8].

These legal issues concerning Internet crime are quite extensive and will not be easily solved. What is legal in one area may not be legal in another area; therefore determining when and where a crime took place can be extremely difficult. Even if a location was identified as the source of the crime, determining the person behind the computer screen, and whether or not it was a state sponsored attack, can be an even harder task.

2.6 Measures of Effectiveness and Past Models

The historical development and nature of the Internet makes securing it very difficult. The Internet was created to allow information to flow freely between trusted users. Today, it is increasingly difficult to determine exactly who has access to what information. The Massachusetts Institute of Technology's Research Program on Communication Policy realized that the original intent of the Internet must be preserved when making security regulations. They outlined four principles that they feel need to be adhered to with regard to information assurance:

1) **Open Architecture:** Policies that permit interconnection among different telecommunications and information systems and services;

2) **Open Access:** Capacity for any subject to enter and compete in the telecommunication and information markets;

3) **Universal Access:** Eliminate physical barriers that hamper general access;

4) **Flexible Access:** Eliminate technical barriers that hamper general access [Valeri, 2000: 133].

While all of these principles may not directly apply to military systems, they do illustrate the tension between competing agendas.

Information assurance that degrades the operational capability of a system to the point where it is no longer useful serves no advantage. The Internet has proved to be too useful a tool to close it off to the world. It is important to keep as much information readily available to the authorized users as possible; placing restrictive security measures across the Internet is not the desired solution. Some systems, however, need to remain secure. It is therefore the goal of this study to provide a model where public information remains accessible and sensitive information remains guarded.

The ever-growing number of security software manufactures prevents product equality. Consumers can never be quite sure that the product they are purchasing is actually doing what the software company claims it can. To combat this problem, the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) collaborated in 1997 to form the National Information Assurance Partnership (NIAP). The NIAP is a "U. S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers" [NAIP: *About*, 2001]. The NIAP Common Criteria Evaluation and Validation Scheme for IT Security is a program that specifically "helps consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace" [NAIP: *Introduction,* 1999]. Forcing software manufacturers to produce quality, secure information technologies on a consistent basis will reduce the number of competitors selling unsatisfactory products.

2.7 Value Focused Thinking

Every organization is different and therefore will have a different perspective on IA, and the impact of IA on its system operational capability and resource costs. Organizations that hold very sensitive information will tend to choose aggressive IA strategies potentially sacrificing operational capability. Likewise, organizations that value the use of the system more than controlling the access and integrity of the information contained in the system will tend to choose IA strategies that minimally impact their operational capability. This is the viewpoint that Value Focused Thinking (VFT) takes in the study, where the values of the decision-maker(s) are captured and consequently pursued, rather than having the decision-maker choose between predetermined lists of alternatives. R. L. Keeney, pioneer of VFT, states, "values are what we fundamentally care about in decision-making. Alternatives are simply means to achieve our values" [Keeney, 1994: 793].

Perhaps the most import element of the decision-making process is to follow a scientific method that will lead to the desired results. The following simple, yet extremely important steps should be followed when making an important and difficult decision:

1) Specify objectives and scales for measuring achievement with respect to those objectives

2) Develop alternatives that potentially might achieve the objective

3) Determine how well each alternative achieves each objective

4) Consider tradeoffs among the objectives

5) Select the alternative that, on balance, best achieves the objectives, taking into account uncertainties [Kirkwood, 1997: 3].

2.7.1 Value Hierarchies

The first step in VFT is to develop a value hierarchy based upon what the decision-maker feels is important to the success of the decision. All value hierarchies must be mutually exclusive and collectively exhaustive [Kirkwood 1997: 17]. Mutual exclusivity in a value hierarchy means that each specific value is only counted once. This prevents a value from being over represented because it is inappropriately counted more than one time. Collectively exhaustive signifies that all the key values of the decision-maker are contained within the model. Failing to represent a value could lead to a decision inconsistent with the decision-maker's true values.

A prototype IA value hierarchy developed by Captain Todd Hamill, USAF, depicted as Figure 2-3 (measures not shown), will be used to illustrate the VFT process from beginning to end. This thesis builds upon Hamill's work and therefore it is beneficial to introduce VFT using his hierarchies as opposed to a notional example.

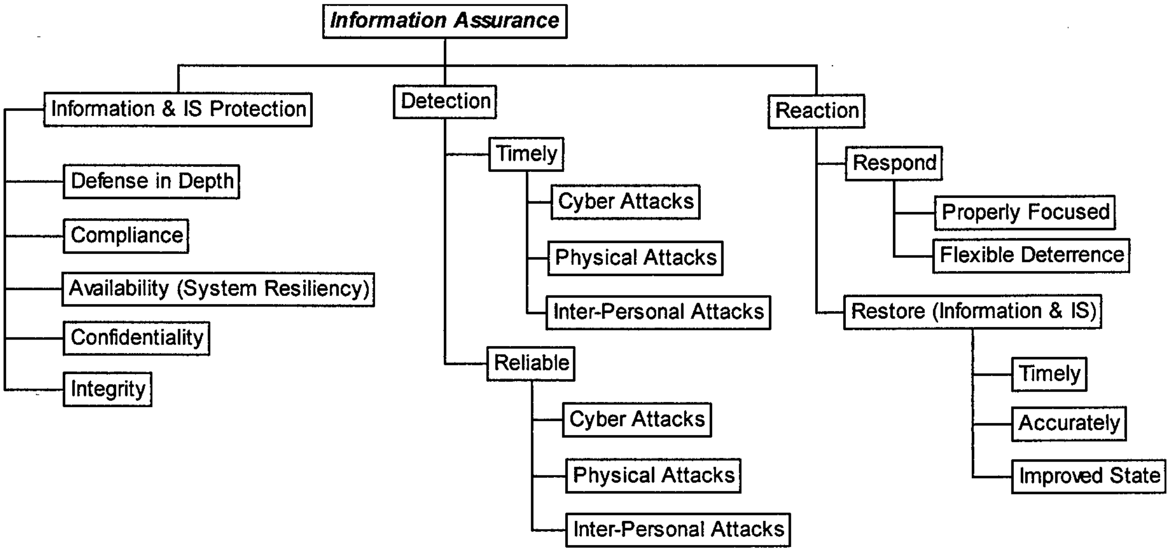


Figure 2-3: Hamill's IA Value Hierarchy [Hamill, 2000: 4-3]

In Hamill's IA hierarchy, the decision-maker's fundamental values in relation to information assurance are Information & Information Systems (IS) Protection, Detection, and Reaction. Since it was determined that Information & Information Systems (IS) Protection, Detection, and Reaction could not be directly measured, they were decomposed until single dimensional, measurable values were obtained. Together, the hierarchy is collectively exhaustive since it captures every key value associated with information assurance (according to this specific decision-maker), and mutually exclusive since no two values are the same.

2.7.2 Value Measures

Once the value hierarchy is established, the decision-maker and analyst again work to establish single dimensional value functions to quantifiably measure each value within the hierarchy. The measure functions are set so that the best possible outcome scores a 1.0 and the worst possible outcome scores a 0.0 [Kirkwood, 1997: 68]. All other outcomes fall somewhere between 0.0 and 1.0. The relationships of the measure functions are required to be either monotonically increasing or decreasing over the range of the value.

Consider the value Integrity found under the Information & Information Systems (IS) Protection column of Hamill's IA hierarchy. In order to determine if a system has integrity, it must be able to be measured. Hamill further decomposed Integrity into Data Integrity and System Integrity. Figure 2-4 illustrates the two measure functions for the value Integrity:

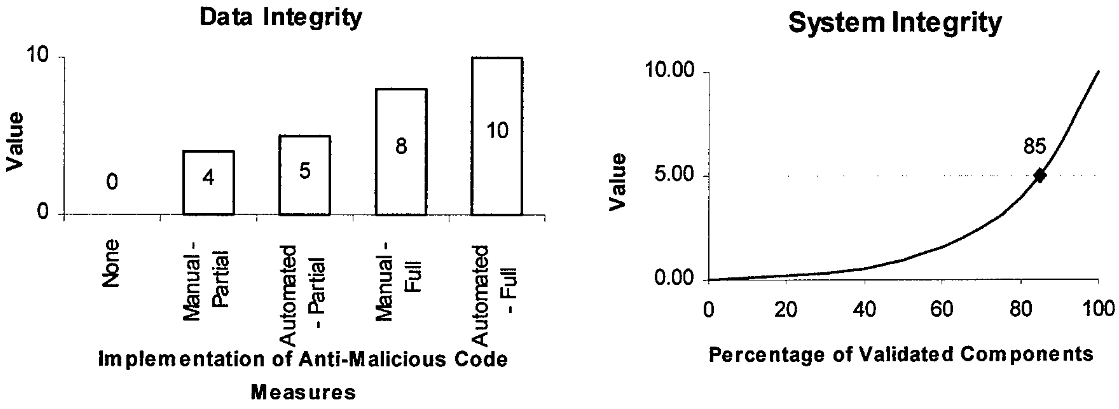


Figure 2-4: Data Integrity Measure [Hamill, 2000: A-34] and System Integrity Measure [Hamill, 2000: A-36]

Measure functions may be categorical, discrete, piecewise linear, or continuous so long as they are monotonic and have non-negative values [Kirkwood, 1997:64-65]. In this example, the value ranges from 0.0 to 10.0, although this may be arbitrary so long as they are consistent. The finalized single dimensional measure functions built in this study and presented in Chapter 3 are on a scale of 0.0 to 1.0.

The exponential mathematical function is used to approximate continuous functions, where ρ (the Greek letter "rho") represents the exponential constant. The exponential single dimensional value function for monotonically increasing preferences, such as shown in the System Integrity graph in Figure 2-4, is given as Equation 2-1:

$$v(x) = \begin{cases} \dfrac{1-\exp[-(x-Low)/\rho]}{1-\exp[-(High-Low)/\rho]}, \rho \neq \infty \\ \dfrac{x-Low}{High-Low}, otherwise \end{cases}$$

Equation 2-1: Monotonically Increasing Exponential Single Dimensional Value Function [Kirkwood, 1997: 65]

The exponential single dimensional value function for monotonically decreasing preferences is given as Equation 2-2:

$$v(x) = \begin{cases} \dfrac{1-\exp[-(High-x)/\rho]}{1-\exp[-(High-Low)/\rho]}, \rho \neq \infty \\ \dfrac{High-x}{High-Low}, otherwise \end{cases}$$

Equation 2-2: Monotonically Decreasing Exponential Single Dimensional Value Function [Kirkwood, 1997: 66]

The value of ρ is determined by measure function's curve. Measures with a large curve will have lower ρ values, and measures with flatter curves will have high ρ values. A perfectly straight line will have a ρ of infinity [Kirkwood, 1997: 65]. Figure 2-5 shows examples of increasing and decreasing exponential single dimensional value functions as ρ is varied:

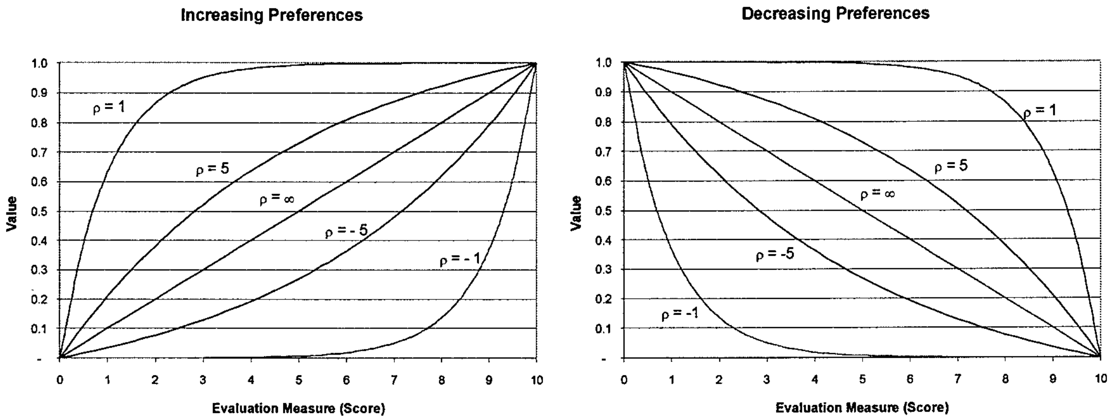


Figure 2-5: Exponential Single Dimensional Value Function Examples [Kirkwood, 1997: 65].

The continuous functions used in this project were approximated using the above equations implemented in a Microsoft Excel © spreadsheet program.

2.7.3 Swing Weighting

Based on the ranges of these functions (its least preferred value to its most preferred value), the decision-maker must weight each measure within the value with respect to all others, then each value within the column, and finally each column within the hierarchy [Kirkwood, 1997: 70]. This establishes a local and a global weight for each value; the local weight is used to measure the importance of the value within the column, and the global weight determines the degree of impact the value will have on an alternative's final value score.

Swing weighting is a technique whereby the "weight for an evaluation measure is equal to the increment in value that is received from moving the score on that evaluation measure from its least preferred level to its most preferred level" [Kirkwood, 1997: 68]. In the example from Hamill's hierarchy, the decision-maker would determine if a change from no Data Integrity (value 0.0) to automated-full Data Integrity (value 1.0) was more or less valuable than a change from 0% System Integrity (value 0.0) to 100% System Integrity (value 1.0). The relative importance of the value increments are compared, and whichever is greater will be weighted accordingly. This technique of comparison weighting, which ultimately produces ratios of relative importance within each tier of the hierarchy, provides a more accurate representation of the decision-maker's true value preferences then weighting without comparison.

For example, suppose the decision-maker determined that the value increment gained by going from 0% System Integrity to 100% System Integrity was three times as important as the value gained by going from no Data Integrity to automated-full Data Integrity. The System Integrity measure would therefore be weighted three times the Data Integrity measure, which on a scale of 0.0 to 1.0, would result in 0.75 and 0.25 respectively. This process would be continued in order to weight Integrity against the other values in the Information and IS Protection column, and then to weight Information and IS Protection, Detection, and Reaction against themselves.

It is essential to remember that the ranges on each measure are the most important factor when determining weights. Generally, the weight of the value will decrease as the range of the value decreases. Suppose a company executive wants to purchase an automobile, and for simplicity's sake, bases his choice of cars on two values: cost and color. Assume that the decision to buy has been made and will not change. When asked to weight these values with respect to each other, most decision-makers would immediately weight cost much higher than color because they believe cost will always be more important. However, if the decision-maker were told that all the cars ranged on cost from $15,000 to $15,100 (a mere $100 difference) then that person may very well weight color above cost since the relative range on cost was so small the decision-maker became essentially indifferent towards the alternatives (with respect to cost). If two cars cost about the same, then the executive would buy the one that came in the color he liked most. Swing weighting captures these scale differences and allows the decision-maker to weight values based on the decision, and not on past prejudices.

2.7.4 Alternative Overall Value Score

After measure functions have been created for each value and assigned their appropriate weight, as determined by decision-maker preferences, strategies can then receive their final overall value score. An alternative's overall value score is calculated by multiplying the global weight of each measure by its respective specific measure value summed across all measures. Equation 2-3 shows this relationship mathematically:

$$v(x) = \sum_{i=1}^{n} \lambda_i v_i(x_i)$$

Equation 2-3: Additive Value Function

Where:

- $\sum_i \lambda_i = 1$ is the requirement for normalization;
- n is the number of objectives (or the number of single dimensional value functions);
- λ_i is the *global* weight for the ith objective;
- $v_i(x_i)$ is the value of the alternative with respect to the ith objective; and,
- $v(x)$ is the overall value of an alternative [Hamill, 2000: 2-31].

2.7.5 Alternative Rankings

The next step of the VFT process after creating and properly weighting the value hierarchy is to determine a Baseline Case to which all other alternatives may be compared. While not necessary in all VFT studies, it was determined that baselining the current system would help to identify value gaps, which are defined to be weaknesses in critical areas in the current operating system. Alternatives can then be tailored to address these value gaps. This is the essence of VFT - creating decision alternatives that address the decision-maker's values. The decision-maker is not forced to choose from a predetermined set of alternatives; they now have the ability to create their own solution guided by their explicitly elicited values. The alternatives are scored based upon measures created to represent each value. Again, every value must have at least one measure so that an alternative may receive a score in that value. The alternative that obtains the highest combined score from Equation 2-3 is therefore the best alternative because it addresses the decision-maker's values better than any other did. If this is not the case, a review of the hierarchy may very well disclose previously unrevealed or missing values and objectives.

A sensitivity analysis can be done on each value weight to see if there is a point where the alternatives will change their rank order. This becomes an important part of the analysis if there are any concerns regarding hierarchy weighting. If the hierarchy is found to be very sensitive, then further analysis may be needed to make certain the weights are correct. Sensitive weights are ones that will reorder alternative rankings if changed within the anticipated possible range of variation. Conversely, insensitive weights are not likely to change the alternatives' rankings, mitigating any concern regarding that particular weight.

Value Focused Thinking was chosen in this study because virtually any properly constructed model can, with care, be fine-tuned and applied to many different organizations. Information assurance is important to every DoD agency and to the civilian sector as well. Assisting decision-makers in improving IA is an essential analysis tool. Decision-makers will value the objectives in the hierarchies differently depending on their particular circumstance; the weighting process allows this differentiation to occur. VFT provides a platform to develop a model that is general enough to be used across a wide spectrum of organizations, yet can be specifically tailored to meet each individual organization's unique mission.

2.8 Past Models

This thesis builds upon previous work presented in a March 2000 Air Force Institute of Technology (AFIT) Master's Thesis effort by Captain Todd Hamill, USAF.

It is a premise of this study that measures of effectiveness be developed in order to quantify the level of IA for a specified organization. Once the organization's current state of IA is determined, different alternatives are then analyzed to show where the most improvement could be gained. However, improving IA impacts system operational capability and resource costs, so it is also necessary to model these elements. The three separate models were used together to analyze AFTAC, as mentioned in Chapter 1. AFTAC is able to see the value that each alternative had with respect to each model, which allows them to have the opportunity to make a final decision as to what, if any, changes they needed to make to their system.

Hamill's information assurance hierarchy originated from the doctrine discussed in previous sections, past AFIT models, and IA experts. The first attempt to model information assurance at AFIT can be found in Captain Michael P. Doyle's et al "*A Value Function Approach to Information Operations MOE's: A Preliminary Study*." Doyle's hierarchy is shown as Figure 2-6.

Although the hierarchy is entitled Defensive Information Operations (IO) and not Information Assurance, the top tier of the hierarchy was derived from the *JP 3-13* definition of IA, which again states that IA must include measures taken to restore "information systems by incorporating protection, detection, and reaction capabilities" [JP 3-13, 1998: I-9]. The hierarchy separates Reaction into Capability Restoration and IO Attack Response.

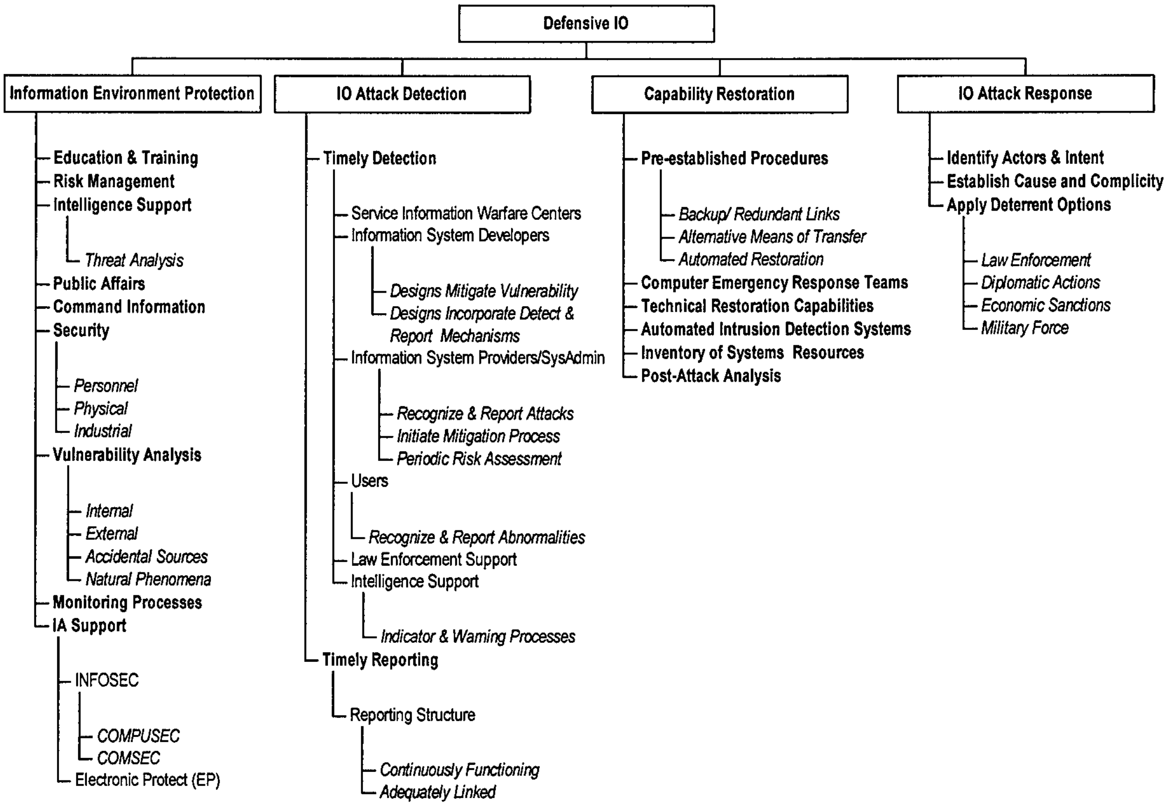


Figure 2-6: Defensive IO [Doyle, Deckro, Jackson, and Kloeber, 1997: 36, JP 3-13, 1998]

Hamill built upon Doyle's research with emphasis on making a model that could be used by a variety of different organizations. Realizing that IA would likely impact the system operational capability and consume resources, Hamill created three separate value hierarchies: Information Assurance, Operational Capability, and Resource Costs. Hamill's hierarchies were used as a starting point to model information assurance at AFTAC, the organization chosen for this study. Figure 2-7 is Hamill's complete IA Value Hierarchy; values are shown in the boxes, with their respective measure functions shown as ovals.

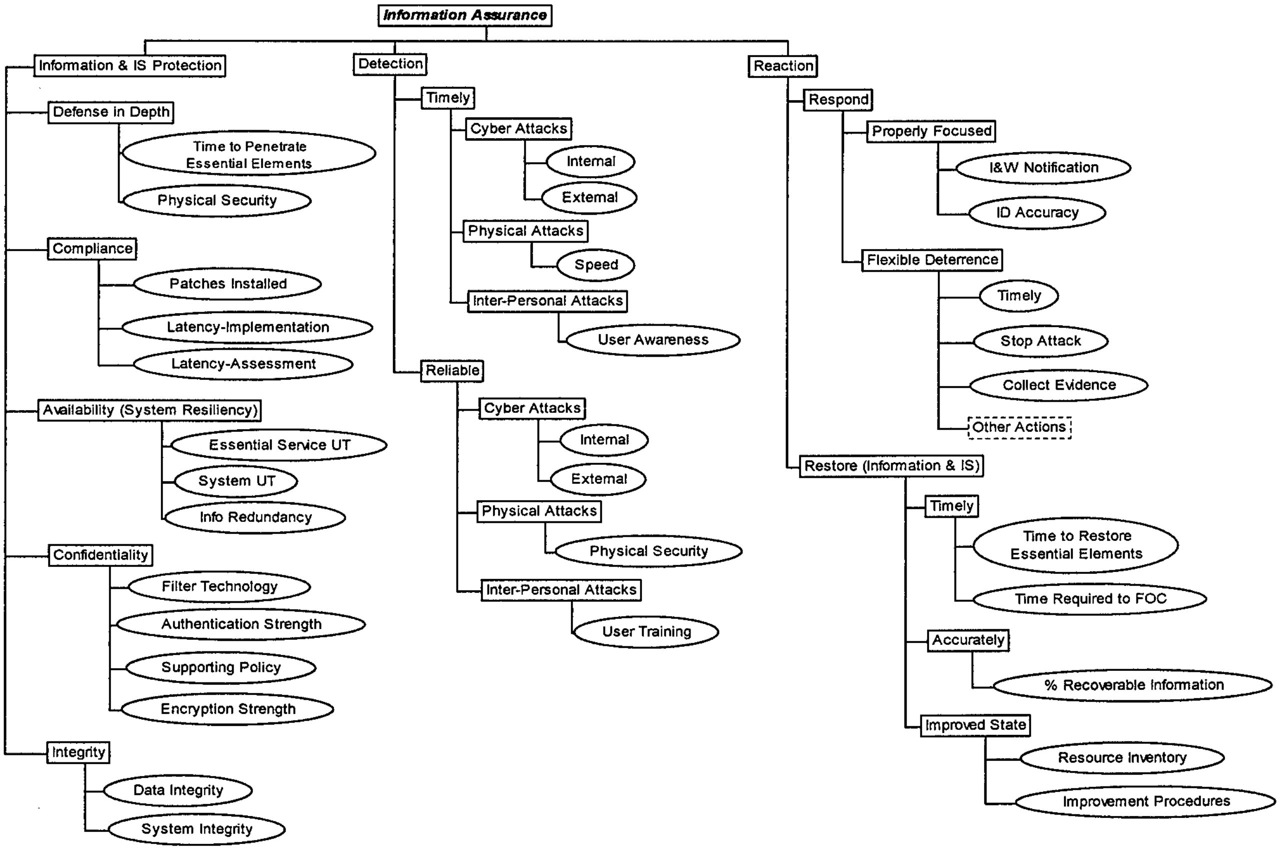


Figure 2-7: Hamill's Information Assurance Value Hierarchy [Hamill, 2000: A-64]

Hamill developed separate models for operational capability and the resource costs of implementing a new IA strategy since information assurance would likely impact them. Figure 2-8 and Figure 2-9 present these value hierarchies along with their associated measures:

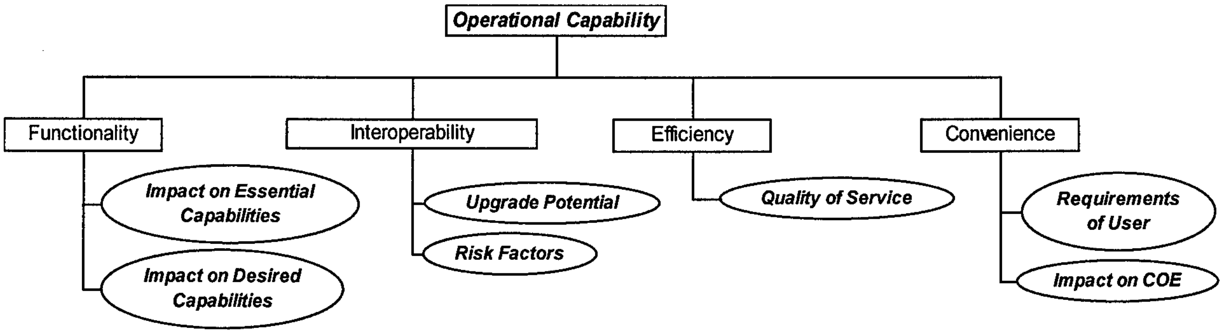


Figure 2-8: Hamill's Operational Capability Value Hierarchy [Hamill, 2000: 4-13]

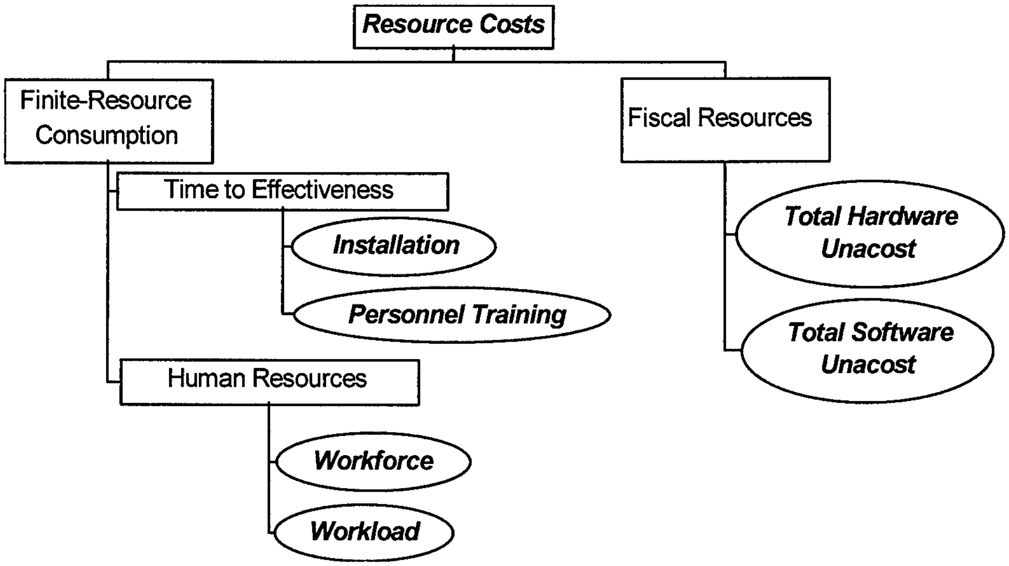


Figure 2-9: Hamill's Resource Costs Value Hierarchy [Hamill, 2000: 4-17]

It is important to note that Hamill's hierarchies were used to aid AFTAC personnel as a starting point in determining how they value information assurance. The hierarchies were not presented as the single, correct manner in which to model information assurance; Chapter 3 will show that the final hierarchies changed significantly. The conceptual models developed by Hamill afford a baseline which, coupled with this study, provides a guide to tailor an IA analysis to a specific organization and system.

2.9 Methodology

This chapter presented a literature review detailing why information assurance is important and some previous attempts to measure it. Chapter 2 also presented a solid theoretical and practical basis for the methodology used to model information assurance at AFTAC, which will be discussed in the following chapter.

3. Methodology

The previous two chapters detailed the importance of Information Assurance and the benefits of developing a quantitative model of IA. However, the models reviewed in Chapter 2 have not been fully tested on operational systems that contain sensitive information. The primary objective of this research was to build on past models, Joint Doctrine, and area experts to develop an IA model that would be applied to an operational system. Hamill's work and joint doctrine provided a solid starting point; however it was not until the values and expertise of IA personnel were captured that the prototype model was fine tuned for a specific operating system. This chapter focuses on the process used to analyze information assurance at AFTAC.

3.1 Model Development

Value Focused Thinking (VFT) was used to develop an Information Assurance Analysis Model. It was determined that measuring the level of IA alone was not sufficient since any IA modifications to a system are highly likely to impact the capability of the system, and the modifications generally cost the organization some amount of resources. The main goal of this thesis is to provide a model that will assist organizations in making IA decisions. In order to accomplish that goal, the entire decision to implement an IA strategy, to include the level of assurance attained, the resource costs consumed by the strategy, and the effects on system operational capability must be considered.

An IA strategy is defined to be either a physical upgrade (hardware, software, or physical security), a change in policy with the intent of improving information assurance, or some combination of the two. The best IA strategies will increase information assurance, increase the system operational capability, and can to be implemented at a low cost to the organization. Figure 3-1 portrays the relationship between Information Assurance (IA), the Impact of Information Assurance on Operational Capability (IOC), and the Impact of Information Assurance on Resource Costs (IRC), with Best Case conditions italicized in the upper right corner of the box.

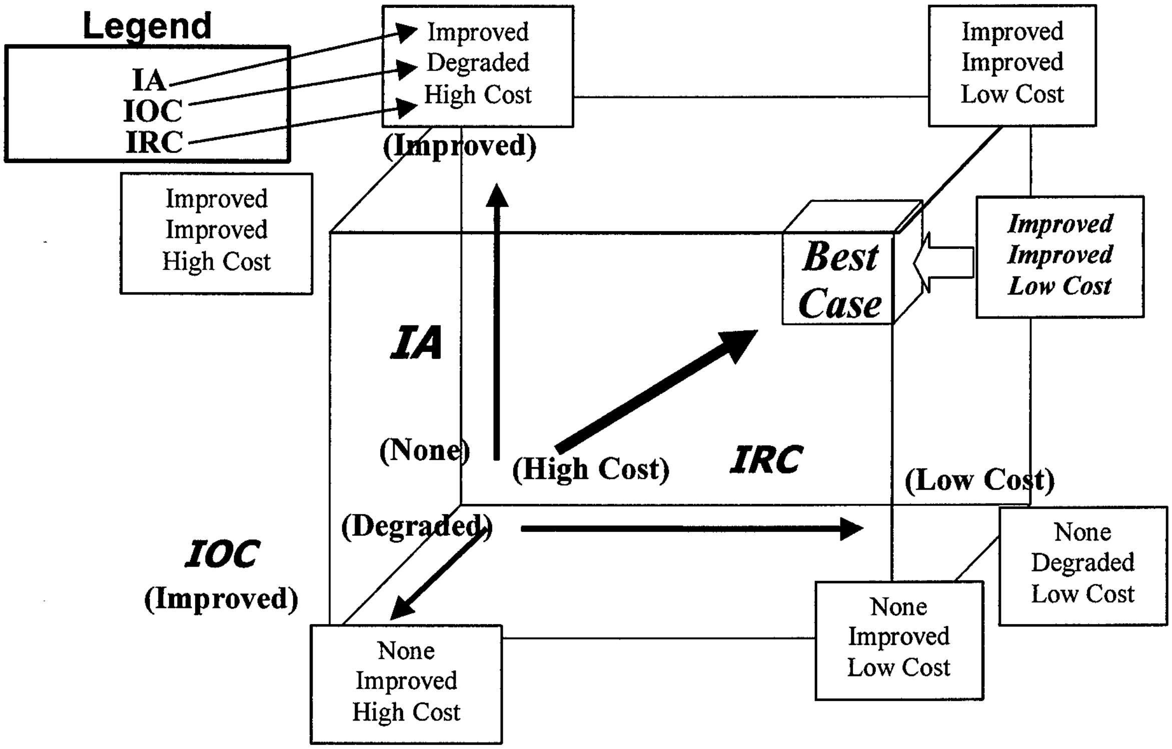


Figure 3-1: The relationship between Information Assurance (IA), the Impact of IA on System Operational Capability (IOC), and the Impact of IA on Resource Costs (IRC) [modified from Hamill, 2000: 4-2]

The model used to measure the decision to implement an IA strategy, the Information Assurance Analysis Model (IAAM), is composed of three separate hierarchies: IA, IOC, and IRC and is shown in Figure 3-2:

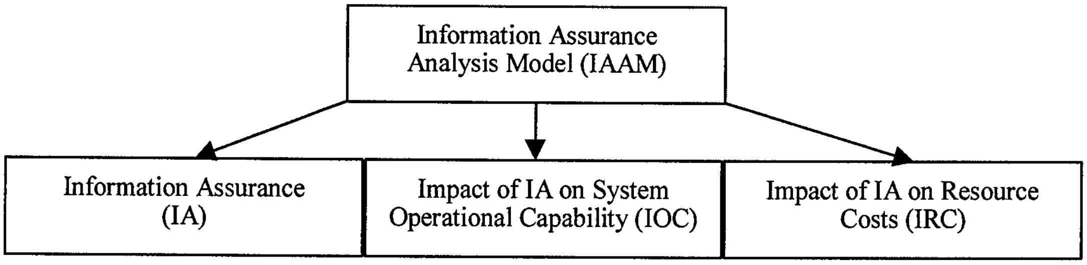

Information Assurance Analysis Model (IAAM)
Information Assurance (IA)
Impact of IA on System Operational Capability (IOC)
Impact of IA on Resource Costs (IRC)

Figure 3-2: Information Assurance Analysis Model (IAAM)

The objective of the IAAM is to assist a decision-maker in determining which, if any, IA strategies should be implemented. The level of information assurance at the organization is captured in the IA hierarchy. It was not the objective of the model to measure overall system operational capability or the current resource costs absorbed by the organization, so these hierarchies do not attempt to do so. The latter two hierarchies simply capture what impact implementing a new IA strategy has on the system operational capability and resource costs, respectively.

The IA, IOC and IRC hierarchies were developed over a series of three separate two to two and a half day meetings with AFTAC / Logistic Support Center (LSC) personnel. Over twenty different information systems experts, including officers, enlisted personnel, civilians, and civilian contractors participated in this study. Expert opinion of all personnel involved with AFTAC information assurance, from senior leadership to technical specialists, was carefully noted and incorporated into the models [AFTAC / LSC, 2000-2001]. This study could not have been completed without the truly extraordinary effort put forth by the AFTAC personnel.

The Information Assurance hierarchy will be discussed first, followed by the Impact of IA on System Operational Capability hierarchy and then the Impact of IA on

Resource Cost hierarchy. A more detailed discussion of each value and its respective measures can be found in the Appendix.

3.2 Information Assurance Value Hierarchy

The IA hierarchy measures the ability of the system and system personnel to assure information, information systems, and information processes. The hierarchy obtains its fundamental focus from the definition of IA found in *JP 3-13: Joint Doctrine for Information Operations:*

> Information assurance is defined as Information Operations (IO) that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities [JP 3-13, 1998: I-9].

Information Assurance is therefore a process that involves the ability to protect information and information systems (IS), detect events that may interfere with information or IS, and properly react to situations where information or IS may have been compromised. The above definition shows that IA is not a synonym for computer security; assurance is a much more robust concept that captures the entire process of defending one's information, information systems, and information processes. Working from *JP 3-13* and the IA experts at AFTAC, it was therefore determined that an IA value hierarchy for AMIS should be composed of protection, detection, and reaction capabilities. The entire IA value hierarchy is given as Figure 3-3, with Information and IS Protection, Detection, and Reaction composing the highest sub-tier of values.

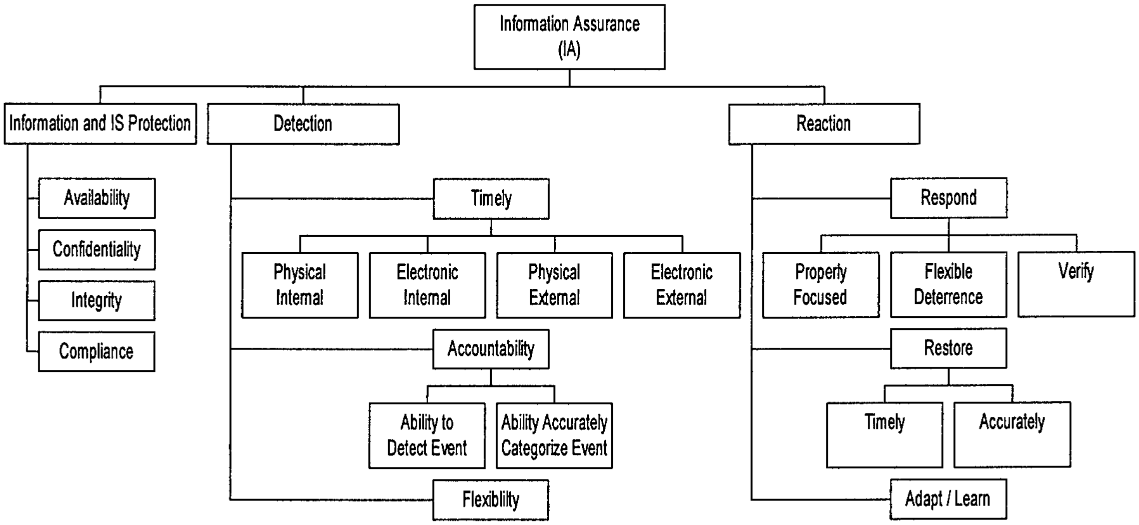


Figure 3-3: Information Assurance (IA) Value Hierarchy

3.2.1 Information and Information Systems (IS) Protection

Information and IS Protection is defined to be the measures taken to ensure that information and information systems are protected from unauthorized change. This includes assuring information and IS availability, confidentiality, and integrity. In addition, AFTAC information assurance experts determined that compliance should also be included under the Information and IS Protection sub-hierarchy since it captures the ability of the system to protect against known vulnerabilities. Each of these sub-hierarchy elements are defined as follows:

Availability: Assured access by authorized users

Confidentiality: Protection from unauthorized disclosure

Integrity: Protection from unauthorized change

Compliance: Measures taken to decrease known vulnerabilities

Single dimensional value functions were developed to measure each of these sub-values. Table 3-1 summarizes the measures used for each value under Information and IS Protection:

Table 3-1: Evaluation Measures for Information and IS Protection

VALUE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Availability	Percentage of E-mail Service Uptime	Percentage (S-Curve)	0	100
	Percentage of Print Service Uptime	Percentage (S-Curve)	0	100
	Percentage of File Service Uptime	Percentage (S-Curve)	0	100
	Percentage of Internet Service Uptime	Percentage (S-Curve)	0	100
Confidentiality	Change in System Confidentiality	Category	Greatly Decreased	Greatly Increased
Integrity	Change in System Integrity	Category	Greatly Decreased	Greatly Increased
Compliance	Percentage of Automated Compliance Procedures	Percentage (Linear)	0	100
	Percentage of Validated Compliance	Percentage (S-Curve)	0	100

* (Shape) of value function, if applicable.

Table 3-1 shows that Availability has four separate single dimensional measure functions since AFTAC personnel valued E-mail, Print, File, and Internet services on AMIS differently. The measure function for Percentage of E-mail Service Uptime is shown in Figure 3-4:

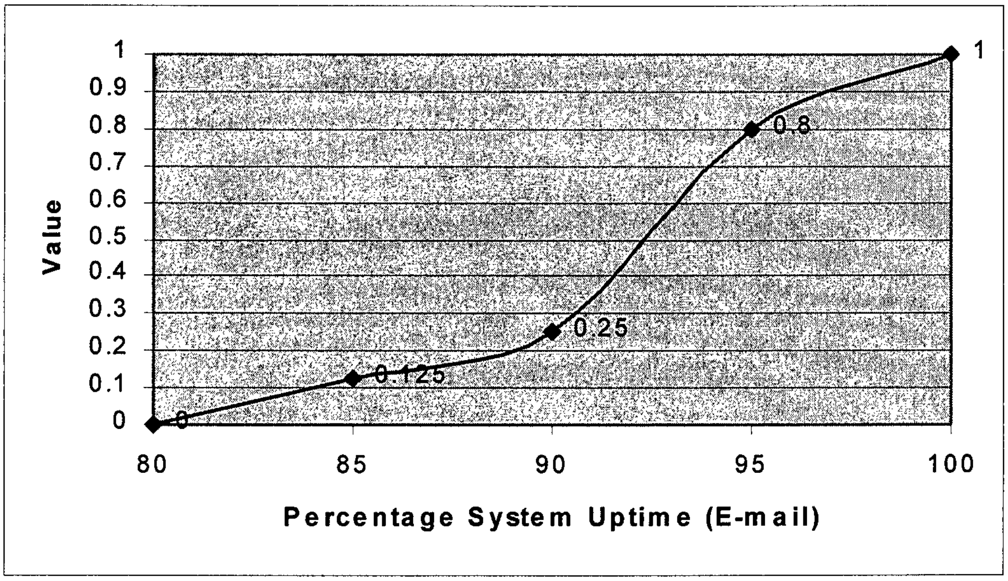


Figure 3-4: Measure function for Percentage of Time E-mail Service is Available

The function is an S-shaped curve ranging from 80% to 100%. Any information assurance strategy that would likely cause E-mail services on AMIS to be available 80% of the time or less would receive a value of 0.0. This value increases slightly until 90% availability, after which it begins to rise sharply. The sharp rise between 90% and 95% availability signifies that AFTAC personnel value gains in this area more than any other of the same magnitude. After 95% availability, AFTAC personnel feel that the service is sufficiently available and therefore any gain above this level is not as valuable, although obviously welcomed. Measure functions, such as shown in Figure 3-4, were also developed for Print, File, and Internet services as well as all other values in the three hierarchies. The complete collection of all values and their associated measure function(s) can be found with a more detailed explanation in the Appendix.

It is important to note that all alternatives, for this hierarchy and for the IRC and IOC hierarchies, were scored in relation to the Baseline Case. This will be discussed in more detail during the discussion on alternative scoring found in Chapter 4.

3.2.2 Detection

Detection is defined to be the ability of the system or system personnel to detect an event. AFTAC personnel defined an event is any abnormal activity or action that could potentially compromise the system or information contained within the system. An event must be detected before any action can be taken. In order for an organization to gain value from their detection capabilities, it must be done quickly, accurately, and at a sufficient level. Detection is therefore separated into three sub-values: Timely, Accountability, and Flexibility.

It is important to detect events as soon as possible since earlier detection will allow earlier reaction, and provide the potential to minimize any negative impact of the event. Although rapid detection is desired for any event, Timely is separated into sub-categories because an IA strategy may have different detection capabilities and needs depending on the method and origin of the event. The categories are composed of either a physical event, which is any event affecting information or information systems originating from a physical source (i.e. a fire), or an electronic event, defined to be an event originating through communication networks. These categories are further separated into events with either internal or external origins, since the organization values their ability to detect events in a timely fashion differently depending on their origin.

Note that whether an event is a result of malicious intent or an accident, it must be detected in a timely manner.

Accountability is defined as the ability of a system to detect and correctly classify events. This value is important because an event that is detected and classified incorrectly, or not at all, could impede the ability of the organization to properly respond. Accountability is separated into the Ability to Detect an Event and the Ability to Classify an Event. The Ability to Detect an Event measures the system or system personnel's ability to determine if an event actually occurred or is occurring. An organization that is able to detect a high percentage of system events will be better able to protect against any possible harm the event may cause. The Ability to Classify an Event captures the ability of the system to correctly classify a detected event. It is important to properly categorize events so that appropriate action may be taken.

Flexibility was defined as the ability to increase or decrease detection fidelity based on the current INFOCON level. AFTAC personnel felt that is would be advantageous to have the ability to adjust its level of assurance based on the current threat level. In a low threat environment, AFTAC would operate at normal assurance levels; as the threat level increases, so does AFTAC's need for information assurance. There is a trade-off that exists between increasing system assurance and operational capability. The consideration of this trade-off is why AFTAC would not necessarily want to operate at the highest possible assurance level in a low threat environment. Table 3-2 summarizes the measures used in the Detection sub-hierarchy:

Table 3-2: Evaluation Measures for Detection

VALUE	SUB-OBJECTIVE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Timely	Physical Internal	Time to Detect a Physical Internal Event	Days (Reverse S-Curve)	0	20
	Electronic Internal	Time to Detect an Electronic Internal Event	Days (Reverse S-Curve)	0	10
	Physical External	Time to Detect a Physical External Event	Hours (Exponential)	0	8
	Electronic External	Time to Detect an Electronic External Event	Minutes (Exponential)	0	120
Accountability	Ability to Detect an Event	Percentage of Automated Detection	Piecewise Linear	0	100
	Ability to Categorize an Event	Percentage of Automated Detection	Piecewise Linear	0	100
Flexibility		Is System Flexible?	Category	No	Yes

* (Shape) of value function, if applicable.

3.2.3 Reaction

Reaction, in this study, is defined to be measures taken to (1) appropriately respond to an identified attack, (2) restore the information and IS capabilities to an acceptable state, their original state, or an improved state, and (3) the ability to learn from previous events so that they do not cause damage in the future. Reaction is thus separated into Respond, Restore, and Adapt. The period after an event is detected is critical to the organization because this is the point at which any potential compromise can be minimized and contained. The manner in which an organization reacts to the event is of high importance since it could determine the extent to which information was compromised.

Respond captures the ability of the system or system personnel to take the proper action during an event or after an event has occurred. It is separated into three values, defined as follows:

> **Timely:** The process of notifying the appropriate personnel after detecting an event, identifying the event source, and then taking the proper action against the event
>
> **Flexible Deterrence:** Taking appropriate action at the appropriate time.
>
> **Verify:** Ability of the system or system administrators to determine if their actions, which include detecting, classifying, and responding to an event, were appropriate.

Restore is defined to be the ability of the system and system personnel to restore information or an information system to an acceptable level after an event. This must be done in both a timely and accurate manner; thus Restore is separated into those respective sub-values. Information must be restored quickly so that system personnel have access to it and are able to use the information to perform their mission. Information that is incorrect, however, has no value to system personnel since processing tainted information could have a severe negative impact on the mission. The restoration of incorrect information is therefore not acceptable.

The final value under the Reaction sub-hierarchy is Adapt / Learn. This is defined to be the ability of the system or system personnel to learn from an event and adapt to the new situations resulting from the event. Part of reacting to an event is learning from that event so it does not occur in the future, and therefore cannot compromise the system again. It is also important that personnel learn from any mistakes made in the assurance process so that they will be better able to control future events. Table 3-3 details the measure functions for the Reaction sub-hierarchy:

Table 3-3: Evaluation Measures for Reaction

VALUE	SUB-OBJECTIVE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Respond	Timely	Time to Notify Support personnel	Proxy (Category)	None	Instantaneous Direct
		Time to Correctly Identify an Event	Hours (Linear)	0	2
		Time to Take Proper Action	Minutes (Linear)	0	60
	Flexible Deterrence	Point at Which Event can be Isolated	Category	System	Event Source
	Verify	Did personnel Detect, Identify, and Act Properly?	Category	No	Yes
Restore	Timely	Time to Restore Full Infrastructure	Hours (Exponential)	0	6
		Time to restore Data	Days (Exponential)	0	5
	Accurately	Percentage of Data Accurately Recovered	Percentage (S-Curve)	20	100
Adapt / Learn		Ability of Support personnel to Teach System	Category	System Cannot be Taught	System can be Fully Taught
		Ability of System to Teach Itself	Category	System Does Not Adapt	System Adapts Automatically

* (Shape) of value function, if applicable.

Again, the Appendix presents a full explanation of the values and associated measure functions.

3.3 The Impact of IA on System Operational Capability

The impact that an information assurance strategy will have on the system's operational capability must be considered when determining what IA strategy or strategies are best for a given organization. The purpose of an information system is to help personnel accomplish their mission in a more efficient manner; if the system cannot do this effectively then it is not a useful system. However, if the user cannot trust that information in the system is available, accurate, updated, and secure, then the user's willingness to depend on the system is greatly decreased. There is a fine balance between information assurance and system operational capability that must exist in order to have a secure but usable system.

In order to isolate the impact of IA on system operational capability, the IOC hierarchy captures only the impact that an IA strategy will have on the system, not the overall system operational capability. Therefore, many of the measures are categorical changes with respect to the baseline system. For example, as shown in Table 3-4, one measure for Efficiency was the Ability to Process Users. This measure was composed of the following categories, all in relation to the Baseline Case: Significantly Decreased, Decreased, No Change, Increased, and Significantly Increased. When the baseline AMIS system was scored, it received a 'No Change' since it did not impact current system efficiency. The Baseline Case scored a 'No Change' for all such IOC measures. Figure 3-5 presents the complete IOC hierarchy:

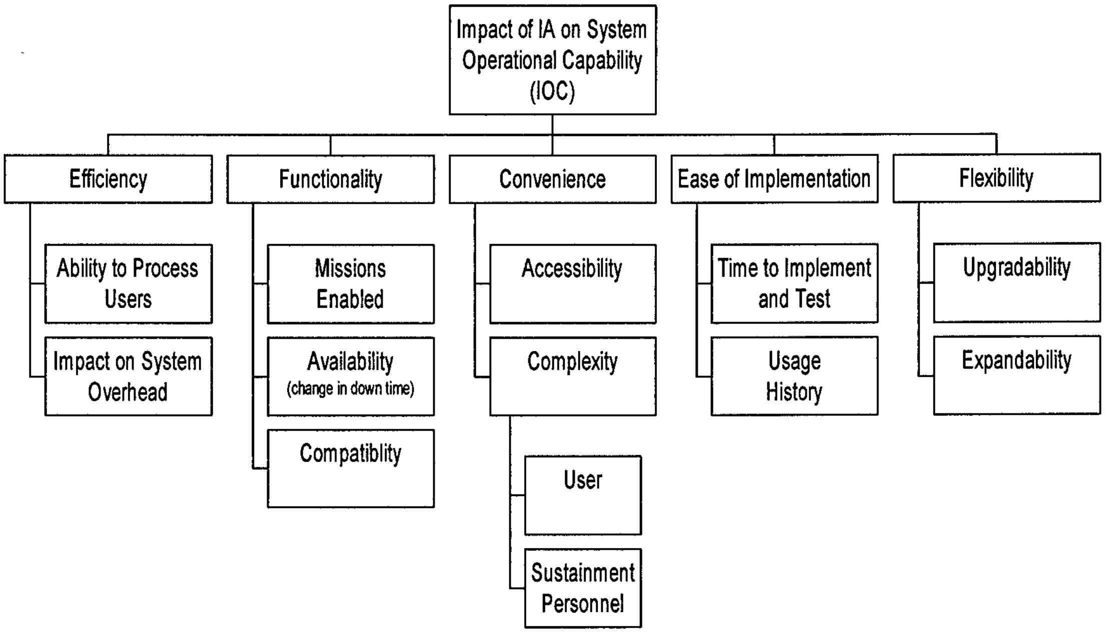


Figure 3-5: Impact of Information Assurance on System Operational Capability (IOC) Value Hierarchy

3.3.1 Efficiency

An efficient system can perform the required tasks quickly and consistently with respect to the demands placed upon the system. It is important that the system is able to process user demands rapidly and without fear of overloading the system. Efficiency is therefore separated into the Ability of the System to Process Users and the Impact an IA strategy will have on System Overhead. The Ability of the System to Process Users is valuable since the system is in place to assist personnel in accomplishing their mission. The speed at which they are able to perform the mission is critical to its success. The impact an IA strategy will have on System Overhead is important because an IA strategy that consumes too much system capacity will limit the system's ability to efficiently process information. Again, these values are not designed to measure the overall system's capabilities; they are designed to measure what impact an IA strategy will have on system capabilities. Measure functions for Efficiency are detailed in Table 3-4:

Table 3-4: Evaluation Measures for Efficiency

VALUE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Ability to Process Users	Change in User Throughput	Category	Significantly Decreased	Significantly Increased
Impact on System Overhead	Change in System Capacity	Category	Significantly Decreased	Significantly Increased
* (Shape) of value function, if applicable.				

3.3.2 Functionality

Functionality is defined as the usefulness offered to system clients by providing information and information related capabilities, both desired and essential. This includes the change in how often the system is Available due to an IA strategy and whether or not the new IA strategy is Compatible with the existing system. Missions Enabled is also included as a value since adding a new capability to the system would increase its functionality. Based on AFTAC personnel expert opinion, it was determined IA strategies that removed a critical mission or function would never be considered for implementation for the system under study. Measure functions for Functionality are explained in Table 3-5:

Table 3-5: Evaluation Measures for Functionality

VALUE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Missions Enabled	Did Strategy enable System to Perform new Mission?	Category	No	Yes
Availability	Change in System Availability	Category	Significantly Decreased	Significantly Increased
Compatibility	Difficulty in Making New Strategy Compatible	Category	Complex	No Difficulty
* (Shape) of value function, if applicable.				

3.3.3 Convenience

Convenience is the level of complication needed to operate the system viewed from both the user and administrator perspective. Convenience is separated into Accessibility, which is the level of difficulty faced by the user in gaining access to authorized systems, and Complexity, defined as the level of difficulty in using the system, again for both for users and support personnel. Complexity was further separated into User and Support Personnel since AFTAC experts deemed that it was far better to have a system that it is easy for users to operate, yet more difficult for support personnel to maintain, than it would be to have an easily maintainable system that was difficult to use. Recall system availability has already been scored in a separate measure and is therefore not considered under Convenience. Table 3-6 explains the measure functions for Convenience:

Table 3-6: Evaluation Measures for Convenience

VALUE	SUB-OBJECTIVE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Accessibility		Degree of Change in System Accessibility	Category	Significantly Decreased	Significantly Increased
Complexity	Users	Degree of Change in User Complexity	Category	Significantly Increased	Significantly Decreased
	Support Personnel (SP)	Degree of Change in SP Complexity	Category	Significantly Increased	Significantly Decreased

* (Shape) of value function, if applicable.

3.3.4 Ease of Implementation

The degree of difficulty associated with installing a new IA strategy is an important consideration when comparing strategies. Ease of Implementation is composed of two separate values: the Time needed to Implement and Test a strategy, and the Usage History of that strategy. The faster an IA strategy can be tested and implemented, the earlier it can begin protecting the system and the less potential disruption it will have on the users. Usage History is the 'track record' of an IA strategy and is important because it gives personnel insight on how well the product or policy fared in the past in similar situations. Usage History contains measures for both the actual history of the product or policy as well as experience system personnel have with using and / or maintaining it. Table 3-7 details measurement functions for the value Ease of Implementation:

Table 3-7: Evaluation Measures for Ease of Implementation

VALUE	SUB-OBJECTIVE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Time to Implement and Test	Software	Time to Implement and Test	Hours (Reverse S-Curve)	0	6
	Hardware	Time to Implement and Test	Days	0	6
	Physical	Time to Implement and Test	Weeks (Reverse S-Curve)	0	4
Usage History		Amount of Exposure Strategy has in Similar Industry	Category	No Exposure	Industry Standard
		Amount of Experience Personnel have with Strategy	Category	No Experience	High Experience

* (Shape) of value function, if applicable.

3.3.5 Flexibility

The final value in the Impact of IA on System Operational Capability is Flexibility, which in this hierarchy is defined to be the ability of the system to change over time as technology evolves. The ability of the system to change with technology is dependent on its ability to be both Upgraded and Expanded, which is captured in the model with those respective values. AFTAC experts determined that Upgradeability and Expandability are binary Yes or No values since there was no clear measure to the degree that all possible strategies are either upgradeable or expandable. This is further explained in the Appendix. Measure functions for Flexibility are explained in Table 3-8:

Table 3-8: Evaluation Measures for Flexibility

VALUE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Upgradeability	Can Strategy be Upgraded?	Category	No	Yes
Expandability	Can Strategy be Expanded?	Category	No	Yes
* (Shape) of value function, if applicable.				

3.4 Impact of IA on Resource Costs

The final consideration when determining what IA strategies to implement is the impact the strategy will have on AFTAC resources. Resources Costs are both the fiscal cost and manpower cost that an IA strategy will require. All other things being equal, the strategy that requires the least amount of AFTAC resources, either financially or with respect to personnel time, will be preferred. The complete IRC value hierarchy is presented as Figure 3-6:

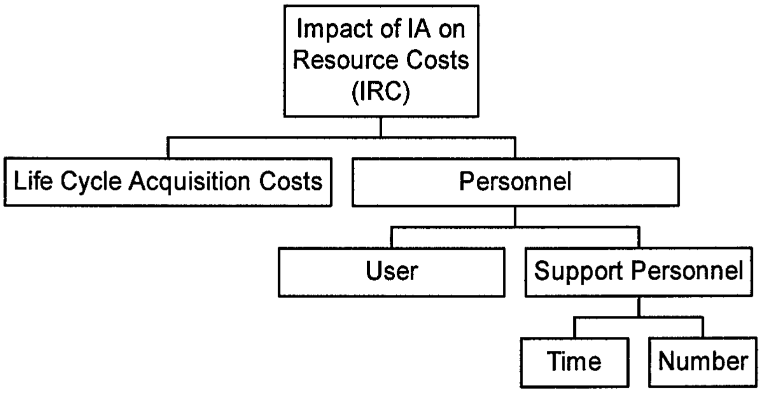

Impact of IA on Resource Costs (IRC)
Life Cycle Acquisition Costs
Personnel
User
Support Personnel
Time
Number

Figure 3-6: Impact of Information Assurance on Resource Costs (IRC) Value Hierarchy

3.4.1 Life Cycle Acquisition Costs

Life Cycle Acquisition Costs is the dollar cost of an IA strategy needed to implement and maintain that strategy over its lifetime. As in any acquisition, an IA strategy that costs the least to acquire, implement, and maintain will be valued higher than more expensive strategies, assuming that they provide an equal amount of assurance. Air Force regulations consider computer system acquisitions differently than other physical acquisitions; therefore they are treated differently in the value measures (again, refer to the Appendix for specific details). Since different IA strategies will have a varying life span, the maintenance costs are normalized to be the average dollar cost per year. Strategies with a projected life span of twenty years can therefore be compared to those with a projected life span of five years. The measure functions for Life Cycle Acquisition Costs are explained in Table 3-9:

Table 3-9: Evaluation Measures for Life Cycle Acquisition Costs

VALUE	SUB-OBJECTIVE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
Life Cycle Acquisition Costs	Initial	Dollar Cost for Computer System	Dollars (Reverse S-Curve)	0	1 million
		Dollar Cost for Physical Construction	Dollars (Reverse S-Curve)	0	5 million
	Recurring	Average Cost of IA Strategy per Year	Dollars (Linear)	0	200,000
* (Shape) of value function, if applicable.					

3.4.2 Personnel

Along with a dollar cost, implementing and maintaining an IA strategy will certainly consume organizational manpower. Users and support personnel are again separated since they are valued differently when considering information assurance strategies, with preference again given to the user. Although information assurance is everyone's duty in the Air Force, user time spent on training in IA or lost due to IA procedures is more valued than support personnel's time spent on IA, since information assurance is not the primary mission of the information system user. It is, however, the job of support personnel to insure that their systems are well assured. Therefore, an IA strategy may impact the number of support personnel needed in addition to the support personnel's time spent on assurance. This is the rationale for separating the value as such. If the strategy automates a process formally done by support personnel, then less support personnel may be needed, which in turn would lower the cost to the organization. Measure functions for the Resource Cost of Personnel is explained in Table 3-10:

Table 3-10: Evaluation Measures for Personnel

VALUE	SUB-OBJECTIVE	MEASURE UNIT	MEASURE TYPE*	LOWER BOUND	UPPER BOUND
User		Time Needed to Train Users	Hours (Reverse S-Curve)	0	4
Support Personnel (SP)	Time	Time Needed to Initially Train SP in Strategy	Days (Reverse S-Curve)	0	20
		Frequency of Training Strategy Requires	Ratio (Piecewise Linear)	Daily	Yearly
		Time per Training Session	Days	0	3
	Number	Percent Change in Necessary SP due to Strategy	Percentage (Reverse S-Curve)	-100	100

* (Shape) of value function, if applicable.

3.5 Weighting

Each value in the hierarchy was weighted using swing weighting. If a value had more than one measure, then each measure was weighted using the same technique. Figure 3-7, Figure 3-8, and Figure 3-9 show the weighted Information Assurance (IA), Impact of IA on System Operational Capability (IOC), and Impact of IA on Resource Cost (IRC) models respectively. Local weights are given above the parenthesized global weights. The local weights for any given tier sum to 1.000 as do the global weights. Note that global weights may not sum to exactly 1.000 due to rounding.

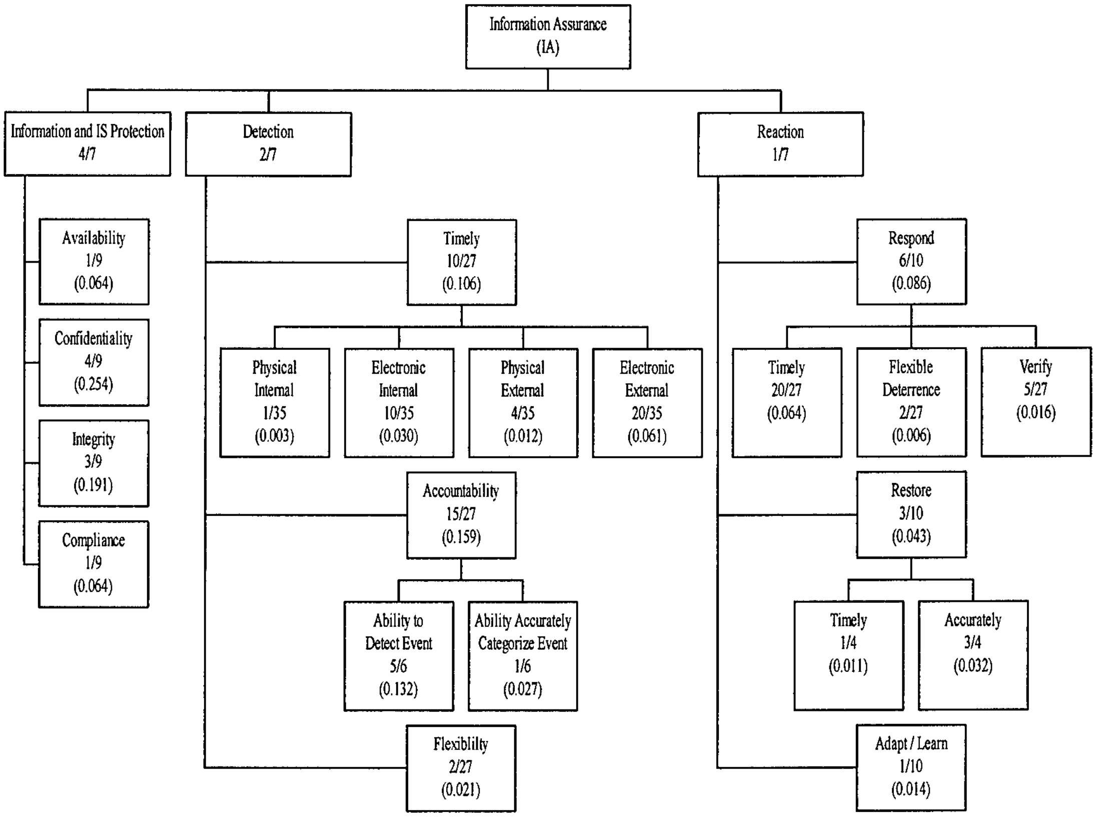

Information Assurance (IA)
Information and IS Protection 4/7
Detection 2/7
Reaction 1/7
Availability 1/9 (0.064)
Confidentiality 4/9 (0.254)
Integrity 3/9 (0.191)
Compliance 1/9 (0.064)
Timely 10/27 (0.106)
Physical Internal 1/35 (0.003)
Electronic Internal 10/35 (0.030)
Physical External 4/35 (0.012)
Electronic External 20/35 (0.061)
Accountability 15/27 (0.159)
Ability to Detect Event 5/6 (0.132)
Ability Accurately Categorize Event 1/6 (0.027)
Flexiblilty 2/27 (0.021)
Respond 6/10 (0.086)
Timely 20/27 (0.064)
Flexible Deterrence 2/27 (0.006)
Verify 5/27 (0.016)
Restore 3/10 (0.043)
Timely 1/4 (0.011)
Accurately 3/4 (0.032)
Adapt / Learn 1/10 (0.014)

Figure 3-7: Weighted Information Assurance Hierarchy, Global Weight in Parentheses

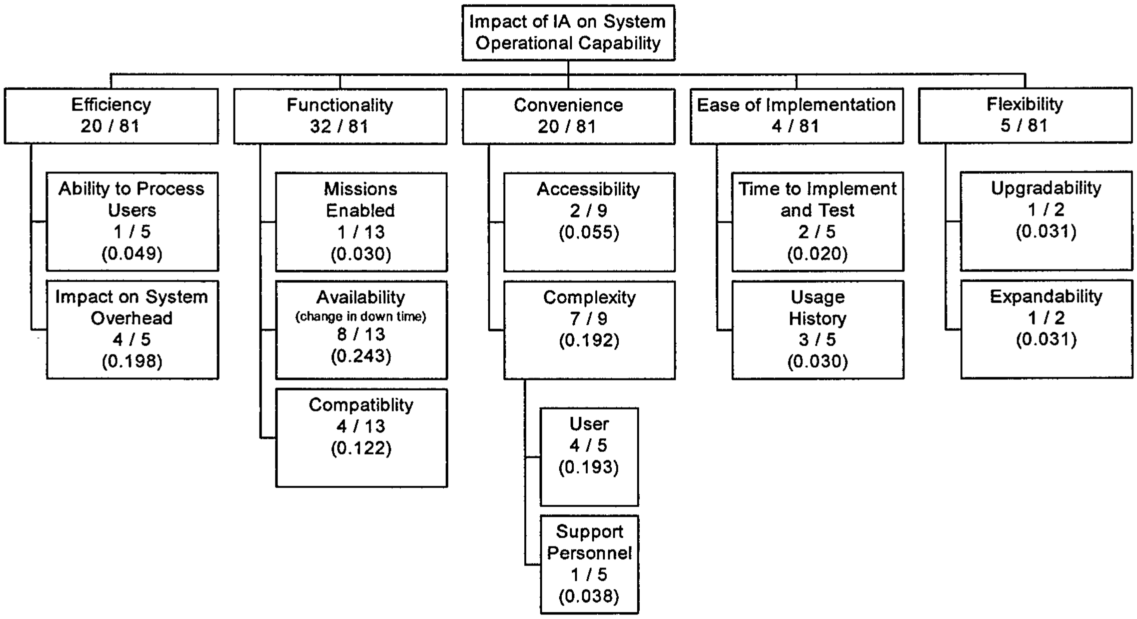

Impact of IA on System Operational Capability
Efficiency 20 / 81
Functionality 32 / 81
Convenience 20 / 81
Ease of Implementation 4 / 81
Flexibility 5 / 81
Ability to Process Users 1 / 5 (0.049)
Impact on System Overhead 4 / 5 (0.198)
Missions Enabled 1 / 13 (0.030)
Availability (change in down time) 8 / 13 (0.243)
Compatiblity 4 / 13 (0.122)
Accessibility 2 / 9 (0.055)
Complexity 7 / 9 (0.192)
User 4 / 5 (0.193)
Support Personnel 1 / 5 (0.038)
Time to Implement and Test 2 / 5 (0.020)
Usage History 3 / 5 (0.030)
Upgradability 1 / 2 (0.031)
Expandability 1 / 2 (0.031)

Figure 3-8: Weighted Impact of IA on Operational Capability Hierarchy, Global Weight in Parentheses

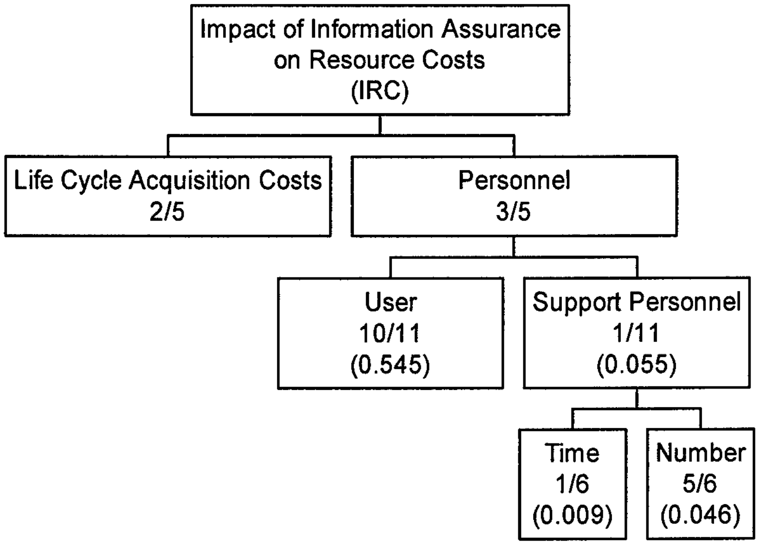

Impact of Information Assurance on Resource Costs (IRC)
Life Cycle Acquisition Costs 2/5
Personnel 3/5
User 10/11 (0.545)
Support Personnel 1/11 (0.055)
Time 1/6 (0.009)
Number 5/6 (0.046)

Figure 3-9: Weighted Impact of IA on Resource Costs Hierarchy, Global Weight in Parentheses

AFTAC information assurance experts weighted the lower tiers of the IA and IOC hierarchies. The top-tier values in the IA and IOC hierarchies were weighted by the commanding officers of the Communications and Information Support Division, to whom the system experts reported. The commanders are the decision-makers ultimately responsible for implementing information assurance strategies. The commanders also weighted the complete IRC hierarchy since the acquisition process is directly under their authority.

3.6 Methodology Summary

This chapter focused on the methodology used to develop, measure, and weight the three separate hierarchies in the Information Assurance Analysis Model (IAAM). Complete details are provided in the Appendix. The IAAM was used to first baseline the system and then to score several information assurance strategies that were being considered by AFTAC for implementation. A sensitivity analysis on the hierarchy weights will be used to show potential changes in alternative rankings. Chapter 4 will discuss the results produced by the model, and provide insight as to how AFTAC can best improve their level of information assurance.

4. Results

The primary objective of this thesis was to provide an information assurance model to an operational Department of Defense (DoD) organization to aid in evaluating and improving their information security. The previous chapter focused on the methodology used to create the Information Assurance Analysis Model (IAAM), which was built in cooperation with the Air Force Technical Applications Center (AFTAC) at Patrick AFB, FL. Recall that the IAAM is composed of three separate hierarchies: Information Assurance (IA), the Impact of IA on System Operational Capability (IOC), and the Impact of IA on Resource Costs (IRC). Together, these three hierarchies were used to evaluate several different information assurance strategies under consideration for implementation into the AFTAC Mission Information System (AMIS), the chosen system for this study. This chapter will analyze the results of each strategy, as well as provide insight as to where AFTAC can best improve their assurance on AMIS. Recall that a detailed description of each measure and its associated single dimensional value function is provided in the Appendix. The Microsoft Excel © spreadsheet model developed as part of this research was used to supplement this analysis.

4.1 The Baseline System

In order evaluate improvements in information assurance on AMIS it was first necessary to measure its current state of IA. Each proposed alternative could then be compared to the current AMIS configuration, the Baseline Case, to determine which course of action would most benefit AFTAC's information assurance. The Baseline Case and all other alternatives were scored exactly as described in the Value Focused Thinking

(VFT) section of Chapter 2. Since AFTAC can choose not to make any modifications to AMIS, the Baseline Case is considered an alternative in this study.

To review, each value within a hierarchy is measured by one or more single dimensional value functions that completely capture the value. For example, under the Information and Information Systems (IS) sub-hierarchy, Availability is a value shown in Figure 4-1:

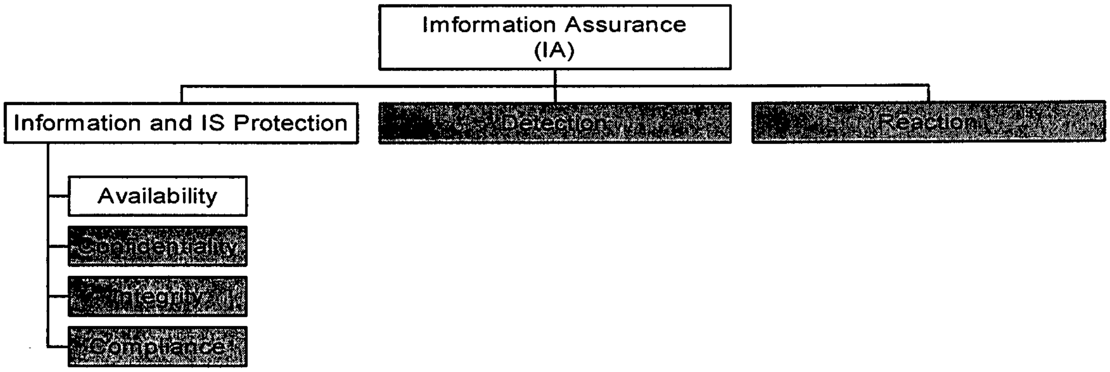


Figure 4-1: Availability

This value is measured by four separate functions: percentage of time E-mail service is available, percentage of time Print service is available, percentage of time File service is available, and percentage of time Internet service is available. The function measuring the percentage of time E-mail Service is available, developed with AFTAC information assurance experts, is shown in Figure 4-2:

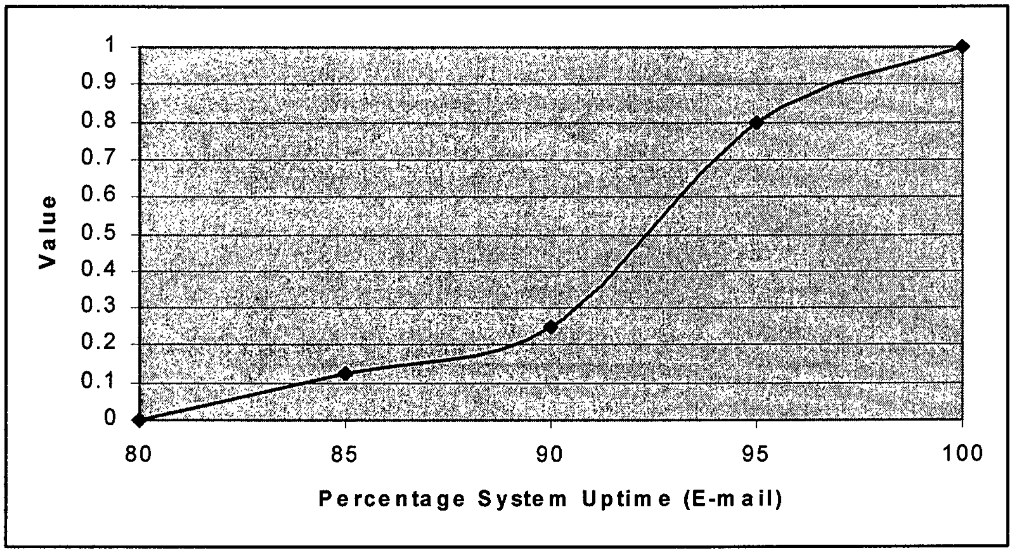


Figure 4-2: Measure function for Percentage of Time E-mail Service is Available

During the scoring session, AFTAC experts were asked to determine what percentage of time E-mail is currently available on AMIS. AFTAC information assurance personnel were shown only the x-axis to each value, and not the actual function itself, to reduce the chance for bias.

Figure 4-3 gives the x-axis for 'Percentage of Time E-mail Service is Available' as it appeared on the scoring sheet used by AFTAC personnel.

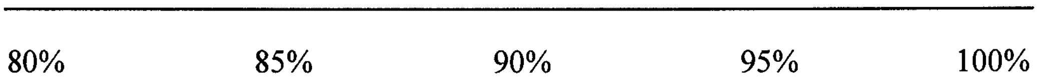


Figure 4-3: X-axis of Percentage of time E-mail Service is Available

AFTAC experts determined that the percentage of time E-mail service was available on the current system was 97%. This score was later converted into a value using the function shown in Figure 4-2. The scoring process was continued using the same x-axis format until all measures in the IAAM model were scored.

Table 4-1 shows the score and corresponding value for each measure under the Information Assurance hierarchy for the Baseline Case. The top-tier values in the hierarchy appear on the left margin of the table, with their respective sub-objectives displayed to the right. Note that not all weights in Tables 4-1 through 4-12 sum to exactly 1.000 due to rounding.

Table 4-1: Scores and corresponding values for each measure in the IA hierarchy – Baseline Case

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Information and IS Protection	Availability		*% Email Service Up Time (UT)*	0.176	0.011	97	0.880
			% Print Service UT	0.176	0.011	99	0.960
			% File Service UT	0.588	0.037	99	0.960
			% Internet Service UT	0.059	0.004	95	0.800
	Confidentiality		*Change in Confidentiality*	1.000	0.254	No Change	0.500
	Integrity		*Change in Integrity*	1.000	0.190	No Change	0.500
	Compliance		*% Automated Compliance Procedures*	0.200	0.012	45	0.451
			% Validated Compliance	0.800	0.051	90	0.900
Detection	Timely	Physical Internal	*Time to Detect*	1.000	0.003	2	0.913
		Electronic Internal	*Time to Detect*	1.000	0.030	3	0.700
		Physical External	*Time to Detect*	1.000	0.012	4	0.167
		Electronic External	*Time to Detect*	1.000	0.060	1	0.950
	Accountability	Ability to Detect Event	*% Automated Detection*	1.000	0.132	80	0.600
		Ability to Categorize Event	*% Automated Detection*	1.000	0.026	75	0.570
	Flexibility		*Is System Flexible?*	1.000	0.021	Yes	1.000
Reaction	Respond	Timely	*Time to Notify Support Personnel (SP)*	0.500	0.032	Instantaneous Indirect	0.900
			Time to Correctly ID Event	0.250	0.016	0.750	0.625
			Time to Take Proper Action	0.250	0.016	15	0.750
		Flexible Deterrence	*Point at Which Event Isolated*	1.000	0.006	Single Server	0.150
		Verify	*Did SP Detect, ID, Act Properly?*	1.000	0.016	Yes	1.000
	Restore	Timely	*Time to Restore Full Infrastructure*	0.500	0.005	1.500	0.625
			Time to Restore Data	0.500	0.005	2.500	0.250
		Accurately	*% Recoverable Information*	1.000	0.032	90	0.417
	Adapt / Learn		*Ability of SP to Teach System*	0.143	0.002	Partially Taught	0.500
			Ability of System to Teach Itself	0.857	0.012	Cannot Adapt	0.000

Overall, the baseline system scored well in the Information Assurance hierarchy receiving a 0.618 out of a possible 1.000. Again, this score is the global weight of each measure multiplied by its associated value, summed across all measures in the hierarchy. The present AMIS system scored well in Availability, where all four measures scored a 0.800 or higher, and Time to Detect Electronic External Events, which received a score of 0.950. Flexibility and Verify both received perfect scores of 1.000, although these measures are weighted significantly less than Availability or Time to Detect Electronic External Events.

It is apparent that several values in the Baseline Case offer potential for improvement. Six of the twenty-five measures scored below a 0.500 out of a possible 1.000: Percentage of Automated Compliance Procedures (0.450), Time to Detect Physical External Events (0.167), Point at which Event is Isolated (0.150), Time to Restore Data (0.250), Percentage of Recoverable Information (0.417), and Ability of System to Teach Itself (0.000). It should be noted that the Baseline Case also scored moderately in Confidentiality and Integrity, each receiving a 0.500. Since these values were measured in relation to the Baseline Case, the Baseline Case itself must receive a 'No Change.' Since Confidentiality and Integrity were the highest weighted measures in the IA hierarchy, with global weights of 0.254 and 0.190 respectively, the effect to the overall IA score was pronounced.

The Baseline Case was also scored against the Impact of IA on System Operational Capability (IOC) and Impact of IA on Resource Costs (IRC) models. Since the IOC hierarchy measured the impact implementing new IA strategies would have on current system operational capability, many of the values scored 'No Change.' This is by design, since there will be no impact on the current system if no IA strategies are implemented. Values that were not measured as a change to the Baseline system were scored to represent the system in its original state. For example, AFTAC experts determined that the usage of current system hardware and software is widespread, therefore the system components were considered to be an 'Industry Standard.' Table 4-2 records the score and corresponding value for each measure under the IOC hierarchy for the Baseline Case:

Table 4-2: Scores and corresponding values for each measure in the IOC hierarchy – Baseline Case

Objective	**Sub-Objective 1**	**Sub-Objective 2**	**Measure**	**Local Weight**	**Global Weight**	**Score**	**Value**
Efficiency	Ability to Process Users		*Change in User Throughput*	1.000	0.049	No Change	0.600
	Impact on System Overhead		*Change in System Capacity*	1.000	0.198	No Change	0.600
Functionality	Missions Enabled		*Did Strategy Enable New Mission?*	1.000	0.030	No	0.000
	Availability		*Change in Availability*	1.000	0.243	No Change	0.900
	Compatibility		*Degree of Difficulty*	1.000	0.122	Simple	0.900
Convenience	Accessibility		*Change in Accessibility*	1.000	0.055	No Change	0.500
	Complexity	User	*Change in User Complexity*	1.000	0.154	No Change	0.500
		Support Personnel (SP)	*Change in SP Complexity*	1.000	0.038	No Change	0.600
Ease of Implementation	Time to Implement and Test		*Software*	0.615	0.012	2	0.800
			Hardware	0.308	0.006	2	0.600
			Physical	0.077	0.002	4	0.000
	Usage History		*Exposure in Similar Industry*	0.200	0.006	Industry Standard	1.000
			SP Experience	0.800	0.024	Moderate Experience	0.550
Flexibility	Upgradeability		*Can System be Upgraded?*	1.000	0.031	Yes	1.000
	Expandability		*Can System be Expanded?*	1.000	0.031	Yes	1.000

The AMIS Baseline Case received a score of 0.698 in the IOC hierarchy. AMIS currently scores well in 'Time to Implement and Test Software' (0.800), fair in 'Time to Implement and Test Hardware' (0.600), and poor in 'Time to Implement Physical Strategies' (0.000). Although 'Time to Implement Physical Strategies' has a global weight of only 0.002, it is an area for improvement. It should be noted, however, that it is an area beyond AFTAC's direct control. The Baseline Case uses 'Industry Standard' IA strategies, and therefore received a score of 1.000 on the 'Exposure in Similar Industry' measure. Improvement could be made in 'Support Personnel Experience with the IA Strategies' however, as this measure received a value score of only a 0.550. All other measures in this hierarchy were designed to capture changes in AFTAC IA strategies, and therefore the Baseline Case scores a 'No Change' in these measures. It is important to note that a score of 'No Change,' in relation to system operational capability, is a desirable score since most IA strategies tend to decrease operational capabilities.

With respect to the Baseline Case, the Impact of IA on Resource Costs model was used to determine the fiscal cost and cost of personnel time. For example, AFTAC cost experts determined that current IA strategies cost approximately $100,000 per year. That number is used as the baseline for the 'Average Cost per Year' measure. Table 4-3 presents the score and corresponding value for each measure under the IRC hierarchy for the Baseline Case:

Table 4-3: Scores and corresponding values for each measure in the IRC hierarchy – Baseline Case

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Life Cycle Acquisition Costs	Initial		*Computer System*	0.333	0.133	0	1.000
			Physical Construction	0.333	0.133	0	1.000
	Recurring		*Normalized Cost per Year*	0.333	0.133	100000	0.500
Personnel	User		*Time Needed to Learn IA Strategy*	1.000	0.545	3	0.100
	Support Personnel (SP)	Time	*Initial Time to Train SP*	0.143	0.001	5	0.600
			Frequency of Training	0.571	0.005	Quarterly	0.500
			Time per Training Session	0.286	0.003	0.250	0.950
		Number	*% Change in SP Needed*	1.000	0.045	0.000	0.700

The Baseline Case scored only a 0.425 in the IRC hierarchy. This low overall IRC score is due, in part, to the undesirable score (0.100) the current AMIS configuration received in User 'Time to Learn IA Strategy.' Since this measure is weighted at 0.545, even a slight improvement in this area would produce a material increase in IRC to AFTAC.

Since the current AMIS configuration has been paid for, and as such is a sunk cost, there is no initial cost to AFTAC to keep the system in its present state. For this reason, the initial costs for 'Computer System' and 'Physical Construction' both received scores of 1.000.

After the Baseline Case was scored, three different information assurance alternatives were scored. These alternatives were IA strategies that were under consideration for implementation on AMIS at the time of this study. When applicable, each measure received a Most Likely Case score, a Best Case score, and a Worst Case score since AFTAC experts were predicting how the system would perform if the strategy were implemented, rather than rating the strategy after implementation. The three strategies considered were Internet Security Scanner (ISS), Enterprise Security Manager (ESM), and Cisco Secure Intrusion Detection System (IDS). It is important to note that these strategies are not necessarily competing with each other; each performs a specific and independent function and thus all three could be implemented simultaneously. They are individually evaluated in the following sections to illustrate how the analysis model can be used.

4.2 Internet Security Scanner (ISS) – Most Likely Case

The Internet Security Scanner is a vulnerability scanner manufactured by Internet Security Systems, Inc. This product would provide AFTAC with the ability to

> Scan network communication services, operating systems, routers, e-mail and Web servers, firewalls, and applications, thereby identifying system weaknesses which could result in unauthorized network access [ISS, 2001].

Table 4-4 details the scores assigned by AFTAC experts based on the Most Likely results from implementing ISS, along with the corresponding value for each measure.

A summary of the Worst Case and Best Case conditions for all alternatives will follow sequentially after the Most Likely Case for each strategy has been presented. It should be noted that all reported scores for ISS, ESM, and Cisco Secure IDS in this section reflect the strategy's contribution to the existing AMIS configuration. The scores are the expected outcome with that specific strategy implemented on the current system, the Baseline Case.

Table 4-4: Scores and corresponding values for each measure in the IA hierarchy – ISS Most Likely Case

Objective	**Sub-Objective 1**	**Sub-Objective 2**	**Measure**	**Local Weight**	**Global Weight**	**Score**	**Value**
Information and IS Protection	Availability		*% Email Service Up Time (UT)*	0.176	0.011	97	0.880
			% Print Service UT	0.176	0.011	99	0.960
			% File Service UT	0.588	0.037	99	0.960
			% Internet Service UT	0.059	0.004	95	0.800
	Confidentiality		*Change in Confidentiality*	1.000	0.254	Increased	0.750
	Integrity		*Change in Integrity*	1.000	0.190	Increased	0.800
	Compliance		*% Automated Compliance Procedures*	0.200	0.012	60	0.601
			% Validated Compliance	0.800	0.051	90	0.900
Detection	Timely	Physical Internal	*Time to Detect*	1.000	0.003	2	0.913
		Electronic Internal	*Time to Detect*	1.000	0.030	3	0.700
		Physical External	*Time to Detect*	1.000	0.012	4	0.167
		Electronic External	*Time to Detect*	1.000	0.060	1	0.950
	Accountability	Ability to Detect Event	*% Automated Detection*	1.000	0.132	80	0.600
		Ability to Categorize Event	*% Automated Detection*	1.000	0.026	75	0.570
	Flexibility		*Is System Flexible?*	1.000	0.021	Yes	1.000
Reaction	Respond	Timely	*Time to Notify Support Personnel (SP)*	0.500	0.032	Instantaneous Indirect	0.900
			Time to Correctly ID Event	0.250	0.016	0.750	0.625
			Time to Take Proper Action	0.250	0.016	15	0.750
		Flexible Deterrence	*Point at Which Event Isolated*	1.000	0.006	Single Server	0.150
		Verify	*Did SP Detect, ID, Act Properly?*	1.000	0.016	Yes	1.000
	Restore	Timely	*Time to Restore Full Infrastructure*	0.500	0.005	1.500	0.625
			Time to Restore Data	0.500	0.005	2.500	0.250
		Accurately	*% Recoverable Information*	1.000	0.032	90	0.417
	Adapt / Learn		*Ability of SP to Teach System*	0.143	0.002	Fully Taught	1.000
			Ability of System to Teach Itself	0.857	0.012	Adapts with SP Help	0.900

AMIS, with the ISS strategy implemented, received an overall score of 0.753 in the IA hierarchy. The reason for the material change over the Baseline Case comes mainly from the Confidentiality and Integrity measures, where ISS received 0.750 and 0.800 respectively. Recall that these measures account for 44.4% of the total possible IA score; therefore any positive change from the Baseline Case results in substantial improvement. With ISS, the number of measures that scored below a 0.500 was reduced to four, with room for improvement still existing in 'Time to Detect Physical External Events,' 'Point at which Event can be Isolated,' 'Time to Restore Data,' and 'Percentage of Recoverable Information.'

The impact to system operational capability caused by installing ISS was considered next. Again, AFTAC experts were asked to score the Most Likely Case, the Best Case, and the Worst Case when applicable. The results for the Most Likely Case are presented in Table 4-5. The IOC hierarchy measures the impact installing an IA strategy will have on the system; all scores are therefore in relation to the Baseline Case presented above.

Table 4-5: Scores and corresponding values for each measure in the IOC hierarchy – ISS Most Likely Case

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Efficiency	Ability to Process Users		*Change in User Throughput*	1.000	0.049	No Change	0.600
	Impact on System Overhead		*Change in System Capacity*	1.000	0.198	Decrease	0.200
Functionality	Missions Enabled		*Did Strategy Enable New Mission?*	1.000	0.030	No	0.000
	Availability		*Change in Availability*	1.000	0.243	No Change	0.900
	Compatibility		*Degree of Difficulty*	1.000	0.122	Simple	0.900
Convenience	Accessibility		*Change in Accessibility*	1.000	0.055	No Change	0.500
	Complexity	User	*Change in User Complexity*	1.000	0.154	No Change	0.500
		Support Personnel (SP)	*Change in SP Complexity*	1.000	0.038	Moderate Increase	0.300
Ease of Implementation	Time to Implement and Test		*Software*	0.615	0.012	2	0.800
			Hardware	0.308	0.006	2	0.600
			Physical	0.077	0.002	4	0.000
	Usage History		*Exposure in Similar Industry*	0.200	0.006	Industry Standard	1.000
			SP Experience	0.800	0.024	Minimal Experience	0.100
Flexibility	Upgradeability		*Can System be Upgraded?*	1.000	0.031	Yes	1.000
	Expandability		*Can System be Expanded?*	1.000	0.031	Yes	1.000

ISS received an overall score of 0.597 in the IOC hierarchy. The strategy scored poorly since personnel believed it would decrease 'System Capacity,' moderately increase 'Support Personnel Complexity,' and because most personnel had limited experience with the product, 'Support Personnel Experience' would also decrease. Combined, these three measures account for about 26% of the total IOC score possible. ISS did not improve over the Baseline Case in any measure in the IOC hierarchy.

Table 4-6 details the impact ISS will have on AFTAC's resource costs. There is no initial cost to purchase ISS since this product can be licensed from Internet Security Systems, Inc. free of charge to AFTAC. However, it will require initial training for AFTAC personnel. Therefore, the cost to train personnel (the majority of which is travel costs) is considered under initial computer systems purchase for all alternatives. Since the objective is to measure the impact on AFTAC resources, all costs were added to the Baseline Case for each alternative. Table 4-6 shows the measure score and corresponding value for the IRC hierarchy for the ISS Most Likely Case.

Table 4-6: Scores and corresponding values for each measure in the IRC hierarchy – ISS Most Likely Case

Objective	**Sub-Objective 1**	**Sub-Objective 2**	**Measure**	**Local Weight**	**Global Weight**	**Score**	**Value**
Life Cycle Acquisition Costs	Initial		*Computer System*	0.333	0.133	0.010	0.990
			Physical Construction	0.333	0.133	0.000	1.000
	Recurring		*Normalized Cost per Year*	0.333	0.133	105000	0.475
Personnel	User		*Time Needed to Learn IA Strategy*	1.000	0.545	3	0.100
	Support Personnel (SP)	Time	*Initial Time to Train SP*	0.143	0.001	7	0.460
			Frequency of Training	0.571	0.005	Quarterly	0.500
			Time per Training Session	0.286	0.003	0.250	0.950
		Number	*% Change in SP Needed*	1.000	0.045	5	0.400

ISS received a score of 0.407 in the IRC hierarchy. Although ISS is relatively inexpensive to maintain, it nonetheless scores worse than the Baseline Case since it is slightly more expensive than maintaining the current system. AFTAC personnel can also expect additional training to learn ISS, which also contributed to lowering ISS's overall IRC score.

While ISS will improve AMIS information assurance, it will do it at a cost to system operational capability and AFTAC resources.

4.3 Enterprise Security Manager (ESM) – Most Likely Case

The Enterprise Security Manager is an Air Force wide information assurance product that is provided at the base level. ESM was formerly manufactured by AXENT Technologies, who merged with the Symantec Corporation, the current product provider. ESM grants the

> ability to automate the planning, management and control of security policy from a single location, thereby saving time and money. [It] does this by giving the ability to off load the repetitive and redundant tasks associated with managing such a policy to computers rather than relying on human staff members [Symantec, 2000].

AFTAC information assurance specialists were again asked to score ESM on the Most Likely Case, the Best Case, and the Worst Case. The Most Likely information assurance provided by the Enterprise Security Manager on AMIS, as determined by AFTAC experts, is shown in Table 4-7. A summary of the results from the Worst and Best Cases will follow after the Most Likely Cases have been presented for each strategy.

Table 4-7: Scores and corresponding values for each measure in the IA hierarchy – ESM Most Likely Case

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Information and IS Protection	Availability		*% Email Service Up Time (UT)*	0.176	0.011	97	0.880
			% Print Service UT	0.176	0.011	99	0.960
			% File Service UT	0.588	0.037	99	0.960
			% Internet Service UT	0.059	0.004	95	0.800
	Confidentiality		*Change in Confidentiality*	1.000	0.254	No Change	0.500
	Integrity		*Change in Integrity*	1.000	0.190	Increased	0.800
	Compliance		*% Automated Compliance Procedures*	0.200	0.012	80	0.801
			% Validated Compliance	0.800	0.051	95	0.950
Detection	Timely	Physical Internal	*Time to Detect*	1.000	0.003	2	0.913
		Electronic Internal	*Time to Detect*	1.000	0.030	3	0.700
		Physical External	*Time to Detect*	1.000	0.012	4	0.167
		Electronic External	*Time to Detect*	1.000	0.060	1	0.950
	Accountability	Ability to Detect Event	*% Automated Detection*	1.000	0.132	80	0.600
		Ability to Categorize Event	*% Automated Detection*	1.000	0.026	75	0.570
	Flexibility		*Is System Flexible?*	1.00	0.021	Yes	1.000
Reaction	Respond	Timely	*Time to Notify Support Personnel (SP)*	0.500	0.032	Instantaneous Indirect	0.900
			Time to Correctly ID Event	0.250	0.016	0.750	0.625
			Time to Take Proper Action	0.250	0.016	15	0.750
		Flexible Deterrence	*Point at Which Event Isolated*	1.000	0.006	Single Server	0.150
		Verify	*Did SP Detect, ID, Act Properly?*	1.000	0.016	Yes	1.000
	Restore	Timely	*Time to Restore Full Infrastructure*	0.500	0.005	1.500	0.625
			Time to Restore Data	0.500	0.005	2.500	0.250
		Accurately	*% Recoverable Information*	1.000	0.032	90	0.417
	Adapt / Learn		*Ability of SP to Teach System*	0.143	0.002	Partially Taught	0.500
			Ability of System to Teach Itself	0.857	0.012	Cannot Adapt	0.000

The ESM strategy scored a 0.683 in the Information Assurance hierarchy, a slight increase over the current system. Part of the reason ESM scored relatively low was that AFTAC personnel believed it would not increase 'Confidentiality,' the single highest weighted measure in the IA hierarchy. ESM is designed to improve system compliance, where it received high scores in both 'Percentage of Automated Compliance Procedures' and 'Percentage of Validated Compliance' measures. However, 'Compliance' was not as heavily weighted. ESM's highly concentrated contribution to IA in Compliance did not have as material an impact as the other strategies.

The most likely projected impact ESM will have on system operational capability is shown in Table 4-8:

Table 4-8: Scores and corresponding values for each measure in the IOC hierarchy – ESM Most Likely Case

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Efficiency	Ability to Process Users		*Change in User Throughput*	1.000	0.049	Decrease	0.200
	Impact on System Overhead		*Change in System Capacity*	1.000	0.198	No Change	0.600
Functionality	Missions Enabled		*Did Strategy Enable New Mission?*	1.000	0.030	No	0.000
	Availability		*Change in Availability*	1.000	0.243	No Change	0.900
	Compatibility		*Degree of Difficulty*	1.000	0.122	Simple	0.900
Convenience	Accessibility		*Change in Accessibility*	1.000	0.055	No Change	0.500
	Complexity	User	*Change in User Complexity*	1.000	0.154	No Change	0.500
		Support Personnel (SP)	*Change in SP Complexity*	1.000	0.038	Minimal Increase	0.450
Ease of Implementation	Time to Implement and Test		*Software*	0.615	0.012	4	0.500
			Hardware	0.308	0.006	2	0.600
			Physical	0.077	0.002	4	0.000
	Usage History		*Exposure in Similar Industry*	0.200	0.006	Industry Standard	1.000
			SP Experience	0.800	0.024	Minimal Experience	0.100
Flexibility	Upgradeability		*Can System be Upgraded?*	1.000	0.031	Yes	1.000
	Expandability		*Can System be Expanded?*	1.000	0.031	Yes	1.000

ESM received an overall IOC score of 0.658. ESM decreased overall IOC because AFTAC experts believed it would slightly decrease 'User Throughput' and minimally increase 'Support Personnel Complexity.' ESM scored exactly as the Baseline Case in all other measures. The impact ESM is projected to have on AFTAC resources is shown in Table 4-9:

Table 4-9: Scores and corresponding values for each measure in the IRC hierarchy –ESM Most Likely

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Life Cycle Acquisition Costs	Initial		*Computer System*	0.333	0.133	0.010	0.990
			Physical Construction	0.333	0.133	0.000	1.000
	Recurring		*Normalized Cost per Year*	0.333	0.133	105000	0.475
Personnel	User		*Time Needed to Learn IA Strategy*	1.000	0.545	3	0.100
	Support Personnel (SP)	Time	*Initial Time to Train SP*	0.143	0.001	6	0.530
			Frequency of Training	0.571	0.005	Quarterly	0.500
			Time per Training Session	0.286	0.003	0.250	0.950
		Number	*% Change in SP Needed*	1.000	0.045	-5	0.800

ESM scored the same as the Baseline system in the IRC hierarchy, with a score of 0.425, implying that the strategy will not add to current AMIS resource costs. The need for improvement in the User 'Time Needed to Learn an IA Strategy' measure remains. ESM is expected to add information assurance to AMIS, while decreasing its operational capability, and leaving resource costs unaffected when the Most Likely Case is considered.

4.4 Cisco Secure Intrusion Detection System (IDS) – Most Likely Case

Formerly known as Cisco NetRanger, the Cisco Secure IDS is a hardware / software intrusion detection device "designed to detect, report, and terminate unauthorized activity throughout a network" [Cisco, 2000]. Table 4-10 presents the most likely projected information assurance results for the Cisco Secure IDS strategy.

Table 4-10: Scores and corresponding values for each measure in the IA hierarchy – Cisco Secure IDS Most Likely Case

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Information and IS Protection	Availability		*% Email Service Up Time (UT)*	0.176	0.011	97	0.880
			% Print Service UT	0.176	0.011	99	0.960
			% File Service UT	0.588	0.037	99	0.960
			% Internet Service UT	0.059	0.004	95	0.800
	Confidentiality		*Change in Confidentiality*	1.000	0.254	Greatly Increased	1.000
	Integrity		*Change in Integrity*	1.000	0.190	Greatly Increased	1.000
	Compliance		*% Automated Compliance Procedures*	0.200	0.012	45	0.451
			% Validated Compliance	0.800	0.051	90	0.900
Detection	Timely	Physical Internal	*Time to Detect*	1.000	0.003	2	0.913
		Electronic Internal	*Time to Detect*	1.000	0.030	3	0.700
		Physical External	*Time to Detect*	1.000	0.012	4	0.167
		Electronic External	*Time to Detect*	1.000	0.060	0.5	0.975
	Accountability	Ability to Detect Event	*% Automated Detection*	1.000	0.132	96	0.920
		Ability to Categorize Event	*% Automated Detection*	1.000	0.026	90	0.828
	Flexibility		*Is System Flexible?*	1.000	0.021	Yes	1.000
Reaction	Respond	Timely	*Time to Notify Support Personnel (SP)*	0.500	0.032	Instantaneous Direct	1.000
			Time to Correctly ID Event	0.250	0.016	0.75	0.625
			Time to Take Proper Action	0.250	0.016	15	0.750
		Flexible Deterrence	*Point at Which Event Isolated*	1.000	0.006	Single Service	0.750
		Verify	*Did SP Detect, ID, Act Properly?*	1.000	0.016	Yes	1.000
	Restore	Timely	*Time to Restore Full Infrastructure*	0.500	0.005	1.5	0.625
			Time to Restore Data	0.500	0.005	2.5	0.250
		Accurately	*% Recoverable Information*	1.000	0.032	90	0.417
	Adapt / Learn		*Ability of SP to Teach System*	0.143	0.002	Fully Taught	1.000
			Ability of System to Teach Itself	0.857	0.012	Adapts with SP Help	0.900

Cisco Secure IDS scored very well in the Information Assurance hierarchy, improving the overall score to a 0.910. The reason Cisco Secure IDS scored well in the IA hierarchy was because it is expected to greatly increase both 'Confidentiality' and 'Integrity.' Receiving a score of 1.000 in each of these measures results in Cisco Secure IDS scoring at least 0.222 higher than the Baseline in their respective overall IA scores. The strategy also has the ability to adapt with personnel help, notify support personnel instantaneously and directly during an event, and scores the same or better in all measures in relation to the Baseline Case.

The Cisco Secure IDS was then scored to determine its impact on system operational capability, as shown in Table 4-11:

Table 4-11: Scores and corresponding values for each measure in the IOC hierarchy – Cisco Secure IDS Most Likely Case

Objective	**Sub-Objective 1**	**Sub-Objective 2**	**Measure**	**Local Weight**	**Global Weight**	**Score**	**Value**
Efficiency	Ability to Process Users		*Change in User Throughput*	1.000	0.049	No Change	0.600
	Impact on System Overhead		*Change in System Capacity*	1.000	0.198	No Change	0.600
Functionality	Missions Enabled		*Did Strategy Enable New Mission?*	1.000	0.030	No	0.000
	Availability		*Change in Availability*	1.000	0.243	Increase	0.950
	Compatibility		*Degree of Difficulty*	1.000	0.122	Moderate	0.600
Convenience	Accessibility		*Change in Accessibility*	1.000	0.055	No Change	0.500
	Complexity	User	*Change in User Complexity*	1.000	0.154	No Change	0.500
		Support Personnel (SP)	*Change in SP Complexity*	1.000	0.038	Moderate Increase	0.300
Ease of Implementation	Time to Implement and Test		*Software*	0.615	0.012	2	0.800
			Hardware	0.308	0.006	2	0.600
			Physical	0.077	0.002	4	0.000
	Usage History		*Exposure in Similar Industry*	0.200	0.006	Industry Standard	1.000
			SP Experience	0.800	0.024	Minimal Experience	0.100
Flexibility	Upgradeability		*Can System be Upgraded?*	1.000	0.031	Yes	1.000
	Expandability		*Can System be Expanded?*	1.000	0.031	Yes	1.000

Although Cisco Secure IDS received the highest IA score, it did not fair as well in IOC, earning a score of a 0.651. It scored lower than the Baseline Case in several measures, taking its most severe decrease in Compatibility's sub-value 'Degree of Difficulty.' It improved upon the Baseline Case in Availability, which helped its IOC score since this measure carried a weight of 0.243.

The projected impact of installing Cisco Secure IDS would have on AFTAC resources is captured in Table 4-12:

Table 4-12: Scores and corresponding values for each measure in the IRC hierarchy – Cisco Secure IDS Most Likely Case

Objective	Sub-Objective 1	Sub-Objective 2	Measure	Local Weight	Global Weight	Score	Value
Life Cycle Acquisition Costs	Initial		*Computer System*	0.333	0.133	0.050	0.950
			Physical Construction	0.333	0.133	0.000	1.000
	Recurring		*Normalized Cost per Year*	0.333	0.133	100000	0.500
Personnel	User		*Time Needed to Learn IA Strategy*	1.000	0.545	3	0.100
	Support Personnel (SP)	Time	*Initial Time to Train SP*	0.143	0.001	15	0.100
			Frequency of Training	0.571	0.005	Quarterly	0.500
			Time per Training Session	0.286	0.003	0.250	0.950
		Number	*% Change in SP Needed*	1.000	0.045	10	0.100

When compared on costs alone, the Cisco Secure IDS strategy is not cost-effective, receiving a score of only 0.391. The strategy's high cost results from its impact on AFTAC Personnel. The User 'Time Needed to Learn an IA Strategy,' 'Initial Time to Train Support Personnel,' and 'Percentage Change in Support Personnel Needed' all scored only a 0.100. Like the other alternatives, the strategy would cost AFTAC a minimal amount of fiscal resources.

Cisco Secure IDS greatly improves the information assurance of AMIS, however it does it at a marginal cost to both system operational capability and AFTAC resources.

4.5 Alternative Comparisons – Most Likely Case

While ISS, ESM, and Cisco Secure IDS could be implemented simultaneously, it is important to determine which alternative would provide the most information assurance to AFTAC. The alternative that ranks highest in each hierarchy will provide the most benefit to the decision-maker for that particular hierarchy. If an alternative ranks above another in one or more hierarchies and the same as another alternative in the remaining hierarchies, then it is said to dominate that alternative. Table 4-13 ranks each alternative with respect to the Information Assurance hierarchy, with the top tier values Information and IS Protection, Detection, and Reaction included. The score of that strategy within the given sub-hierarchy is given in parentheses.

Table 4-13: Alternative Rankings and Scores with respect to IA – Most Likely Case

Alternative	**Information and IS Protection (max = 0.571)**	**Detection (max = 0.286)**	**Reaction (max = 0.143)**	**Overall Information Assurance Score (max = 1.00)**
Baseline	4 (0.333)	tie – 2 (0.199)	tie – 3 (0.086)	4 (0.618)
ISS Most Likely	2 (0.456)	tie – 2 (0.199)	2 (0.098)	2 (0.753)
ESM Most Likely	3 (0.397)	tie – 2 (0.199)	tie – 3 (0.086)	3 (0.683)
Cisco Secure IDS Most Likely	1 (0.555)	1 (0.250)	1 (0.105)	1 (0.910)

Table 4-13 shows that with respect to Information Assurance alone, Cisco Secure IDS Most Likely outcome dominates all other alternatives. Clearly, Cisco Secure IDS will provide AMIS with the highest level of information assurance among the alternatives evaluated, scoring 0.910 out of a possible 1.000. ISS and ESM will each also increase the current level of information assurance on AMIS, although to a lesser degree than Cisco Secure IDS.

Figure 4-4 is a graphical representation of Table 4-13. The Best Possible Case is displayed at the top of Figure 4-4 to illustrate the maximum possible attainable score in Information and IS Protection, Detection, Reaction, and Overall Information Assurance. The chart shows Cisco Secure IDS does substantially better than the other alternatives in Information and IS Protection, Detection, and Reaction, resulting in it being the overwhelming choice for best IA strategy.

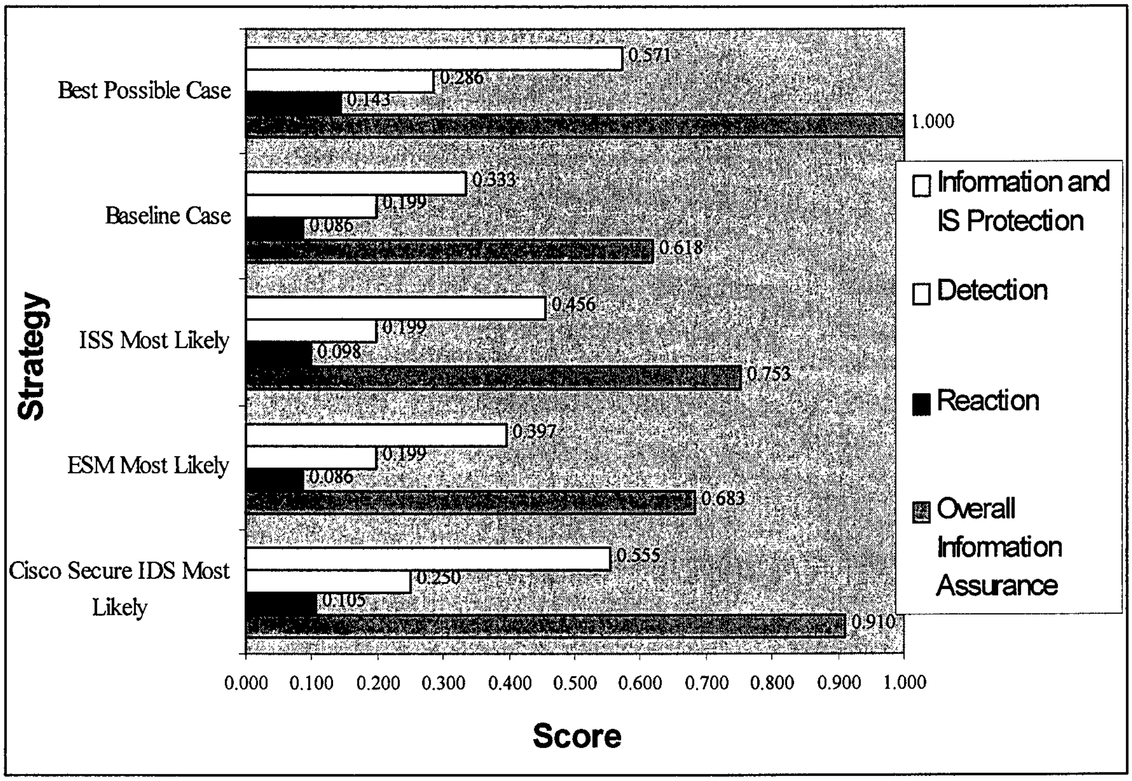


Figure 4-4: Alternative Comparisons with respect to IA - Most Likely Case

However, information assurance is only one part of the Information Assurance Analysis Model (IAAM). Table 4-14 shows the alternative rankings for the Impact of IA on System Operational Capability Model, again with the top tier values shown:

Table 4-14: Alternative Rankings and Scores with respect to IOC – Most Likely Case

Alternative	Efficiency (max = 0.247)	Functionality (max = 0.395)	Convenience (max = 0.247)	Ease of Implementation (max = 0.049)	Flexibility (max = 0.062)	Overall IOC Score (max = 1.00)
Baseline	tie – 1 (0.148)	tie – 1 (0.328)	1 (0.127)	1 (0.032)	tie – 1 (0.062)	1 (0.698)
ISS Most Likely	4 (0.069)	tie – 1 (0.328)	tie – 3 (0.116)	tie – 2 (0.022)	tie – 1 (0.062)	4 (0.597)
ESM Most Likely	3 (0.128)	tie – 1 (0.328)	2 (0.122)	4 (0.018)	tie – 1 (0.062)	2 (0.658)
Cisco Secure IDS Most Likely	tie – 1 (0.148)	4 (0.304)	tie – 3 (0.116)	tie – 2 (0.022)	tie – 1 (0.062)	3 (0.651)

Not surprisingly, the Baseline Case is the preferred alternative when considering the impact IA strategies will have on system operational capability. Each additional strategy was measured based on its impact or change to the current state. The Cisco Secure IDS Most Likely alternative, which was clearly the best alternative with respect to information assurance alone, scored only slightly lower (0.658 to 0.651) than the ESM Most Likely Case in overall IRC. Figure 4-5 is a graphical representation of Table 4-14.

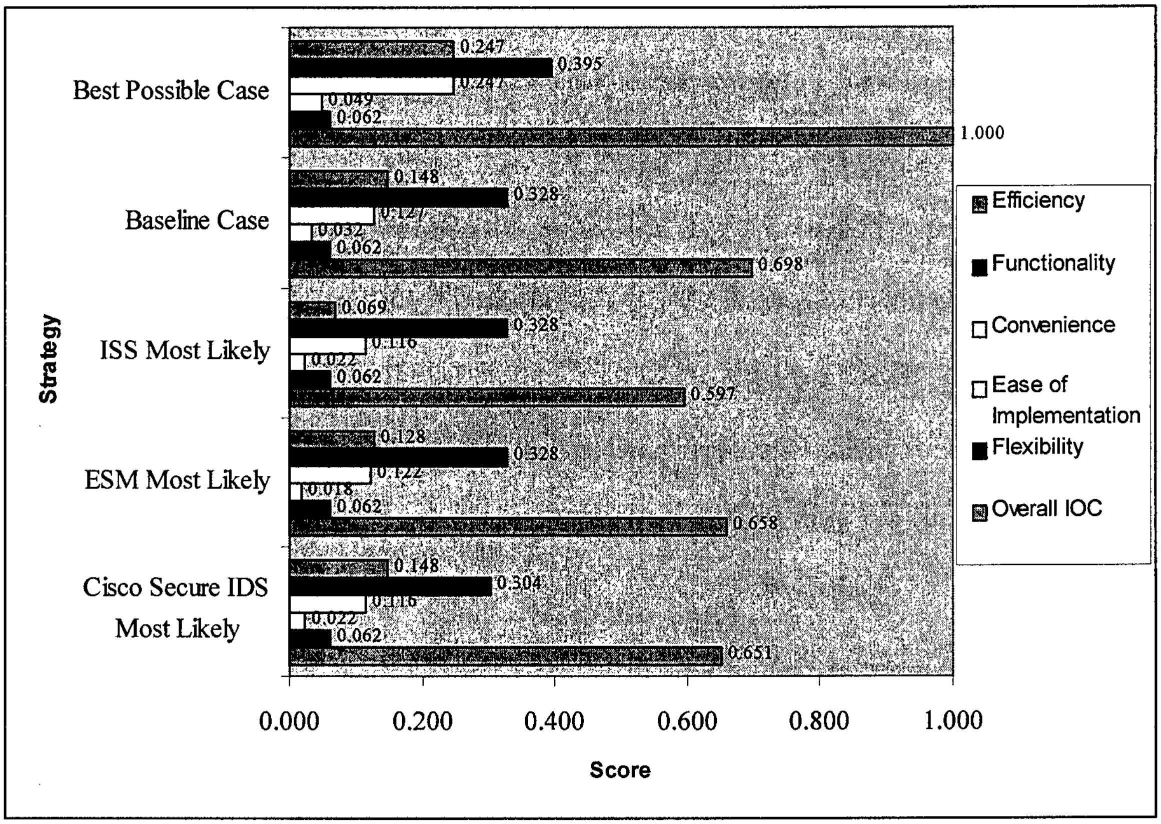


Figure 4-5: Alternative Comparisons with respect to IOC - Most Likely Case

Figure 4-5 shows that Cisco Secure IDS was higher than ESM in Efficiency (by 0.020), slightly lower than ESM in Functionality (by 0.024), and virtually even in Convenience, Ease of Implementation, and Flexibility.

Table 4-15 presents the results of the four alternatives with respect to the Impact of Information Assurance on Resource Costs hierarchy, with the respective rank again parenthesized:

Table 4-15: Alternative Rankings and Scores with respect to IRC – Most Likely Case

Alternative	**Life Cycle Acquisition Costs (max = 0.40)**	**Personnel (max = 0.60)**	**Overall IRC Score (max = 1.00)**
Baseline	1 (0.333)	2 (0.092)	Tie – 1 (0.425)
ISS Most Likely	tie – 2 (0.329)	3 (0.078)	3 (0.407)
ESM Most Likely	tie – 2 (0.329)	1 (0.097)	Tie – 1 (0.425)
Cisco Secure IDS Most Likely	4 (0.327)	4 (0.064)	4 (0.391)

The Baseline Case and ESM Most Likely tie as the top alternative with respect to the Impact of an IA on AFTAC Resource Costs hierarchy. Table 4-15 shows that while the Baseline is less expensive to maintain (hence the higher value), the ESM Most Likely alternative requires less personnel. It should be noted that the maximum value possible for Personnel is 0.600 yet no alternative reached 0.100. This is clearly a value gap in the set of alternatives. Developing a new alternative that could produce a high score on the Personnel value would greatly improve the overall IRC score. A graphical representation of Table 4-15 is given as Figure 4-6:

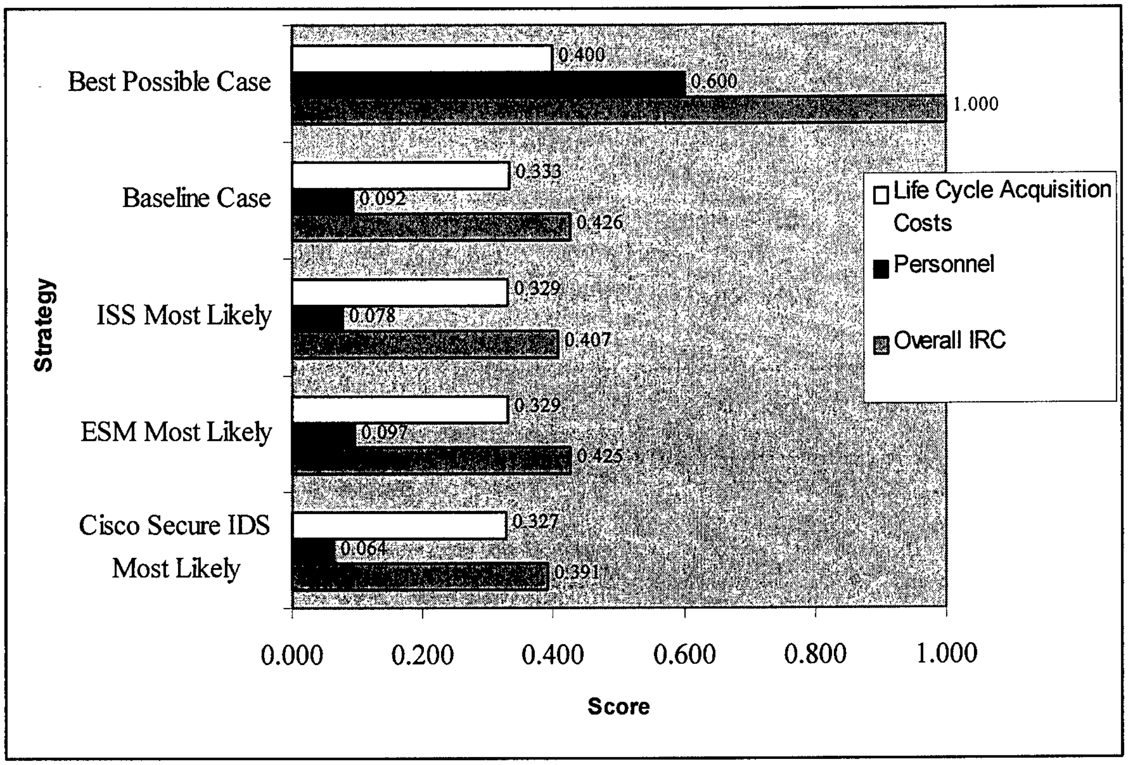


Figure 4-6: Alternative Comparisons with respect to IRC - Most Likely Case

Table 4-16 gives a summary of the alternatives and their respective rank within each hierarchy. No alternative dominated another.

Table 4-16: Summary of Alternative Rankings – Most Likely Case

Alternative	Information Assurance Rank	IOC Rank	IRC Rank
Baseline	4	1	1
ISS Most Likely	2	4	3
ESM Most Likely	3	2	1
Cisco Secure IDS Most Likely	1	3	4

Figure 4-7 presents the Most Likely strategy results on the three IAAM hierarchies. Again note that Cisco Secure IDS is clearly the best alternative with respect to Information Assurance, however the IOC and IRC hierarchies display a much tighter range.

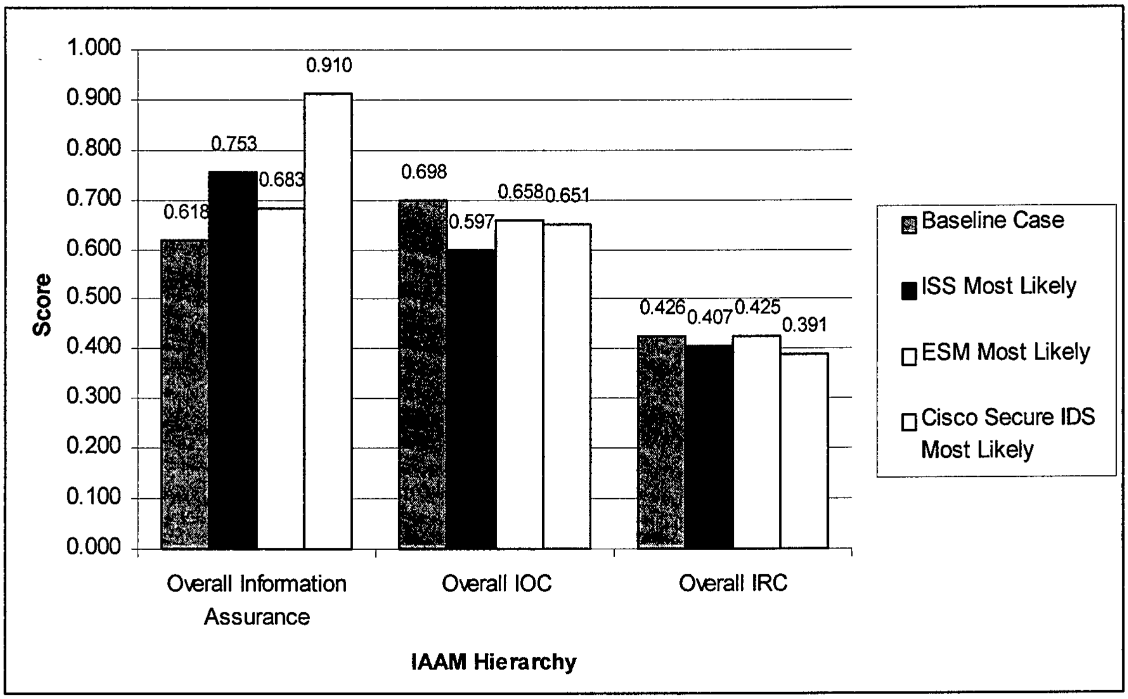


Figure 4-7: Most Likely Case Results, Separated by IAAM Hierarchy

Presented with these alternatives, the decision-maker(s) could now consider the relative merits of each alternative given their scores in each of the three hierarchies. As was seen in the preceding analysis, the total measures can be "peeled-back" to any level of the hierarchy to reveal the sources of the differences. The decision-maker's values can help clarify differences in the alternatives and allow him or her to use their expertise to make the final selections. The associated analysis is available to support the decision-maker's expertise.

A summary of the Most Likely conditions is given as a radar chart in Figure 4-8. Each axis of the chart represents one of the hierarchies in the IAAM. The higher a strategy scores in any given hierarchy, the further out its representative line will be on that specific axis. This chart shows that Cisco Secure IDS is the clear winner in the Information Assurance hierarchy. The strategies are tightly grouped in both the IRC and

IRC hierarchies, indicating that the Cisco Secure IDS would not substantially change system operational capability or consume large amounts of AFTAC resources. It has been shown, however, that Cisco Secure IDS is slightly outperformed in IOC and IRC. The decision-maker will need to consider the relative merits of each value when making a final decision.

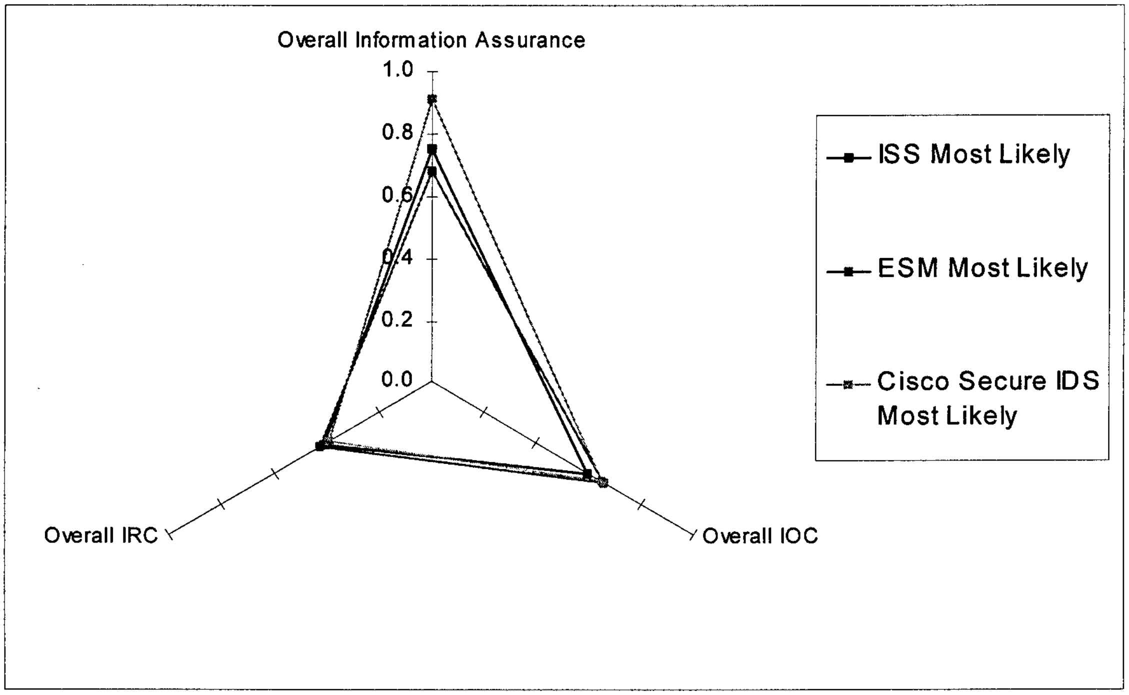


Figure 4-8: Radar Chart on Most Likely Case Results

4.6 Worst and Best Case Comparisons

While the analysis of the Most Likely Case provided insight, it is important to consider potential "downside" risk and "upside" gains since the information assurance strategies may not perform exactly as specified. For this reason, the Internet Security Scanner, Enterprise Security Manager, and Cisco Secure IDS were also scored on a Worst Case and a Best Case conditions for each appropriate measure. Any measure that

AFTAC personnel felt would not vary was left as it was originally scored. A summary of the results from the Worst and Base Case conditions is presented in the following sections.

4.6.1 Alternative Comparisons – Worst Case Conditions

The Worst Case conditions for each alternative and the Baseline are summarized in the following tables. Since AFTAC personnel cannot select whether a strategy performs as expected, the Worst Case conditions are only compared to one another. The Baseline Case, which did not change, is provided as a reference. Table 4-17 provides the score and associated rank for each Worst Case alternative with respect to the Information Assurance hierarchy, with Information and IS Protection, Detection, and Reaction separated:

Table 4-17: Alternative Rankings and Scores with respect to IA – Worst Case

Alternative	Information and IS Protection (max = 0.571)	Detection (max = 0.286)	Reaction (max = 0.143)	Overall Information Assurance Score (max = 1.00)
Baseline	4 (0.333)	tie – 2 (0.199)	tie – 3 (0.086)	4 (0.618)
ISS Worst Case	3 (0.334)	tie – 2 (0.199)	2 (0.098)	2 (0.631)
ESM Worst Case	2 (0.336)	tie – 2 (0.199)	tie – 3 (0.086)	3 (0.622)
Cisco Secure IDS Worst Case	1 (0.555)	1 (0.250)	1 (0.105)	1 (0.910)

The Cisco Secure IDS Worst Case is the same as its Most Likely Case with respect to Information Assurance. Since there is no variation for Cisco Secure IDS on IA, and it was the highest ranked alternative with respect to the Most Likely outcome, it is guaranteed to produce the highest amount of assurance of any alternative. Figure 4-9 is a graphical representation of Table 4-17.

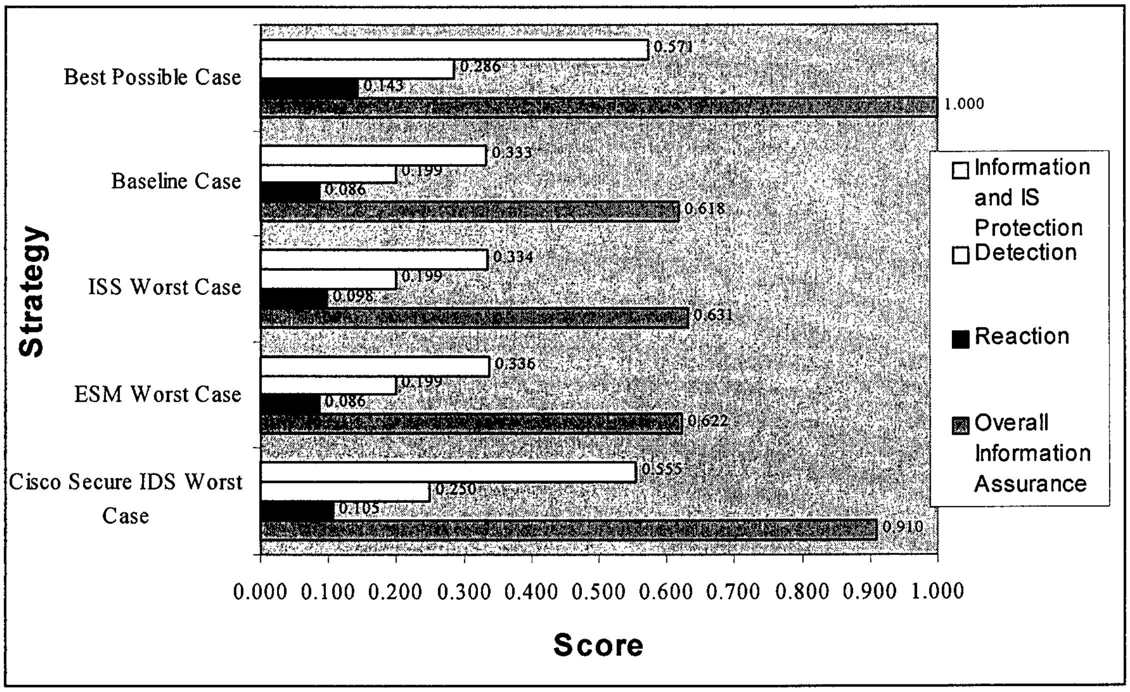


Figure 4-9: Alternative Comparisons with respect to IA - Worst Case

In the Worst Case conditions, ISS and ESM lose substantial value in Information and IS Protection, while Cisco Secure IDS is able to maintain its Most Likely score. Table 4-18 summarizes the rankings with respect to the IOC model:

Table 4-18: Alternative Rankings and Scores with respect to IOC – Worst Case

Alternative	**Efficiency (max = 0.247)**	**Functionality (max = 0.395)**	**Convenience (max = 0.247)**	**Ease of Implementation (max = 0.049)**	**Flexibility (max = 0.062)**	**Overall IOC Score (max = 1.00)**
Baseline	tie – 1 (0.148)	tie – 1 (0.328)	1 (0.127)	1 (0.032)	tie – 1 (0.062)	1 (0.698)
ISS Worst Case	tie – 3 (0.049)	4 (0.049)	tie – 3 (0.116)	3 (0.019)	tie – 1 0.062	4 (0.295)
ESM Worst Case	tie – 3 (0.049)	tie – 1 (0.328)	2 (0.122)	4 (0.010)	tie – 1 (0.062)	3 (0.570)
Cisco Secure IDS Worst Case	tie – 1 (0.148)	2 (0.304)	tie – 3 (0.116)	2 (0.020)	tie - 1 (0.062)	2 (0.650)

Table 4-18 shows that if the Worst Case conditions occurred for every alternative, Cisco Secure IDS would improve to second best behind only the Baseline Case. If the Worst

Case occurred for ISS, AFATC would experience a severe loss in system operational capability. Figure 4-10 is a graphical representation of Table 4-18:

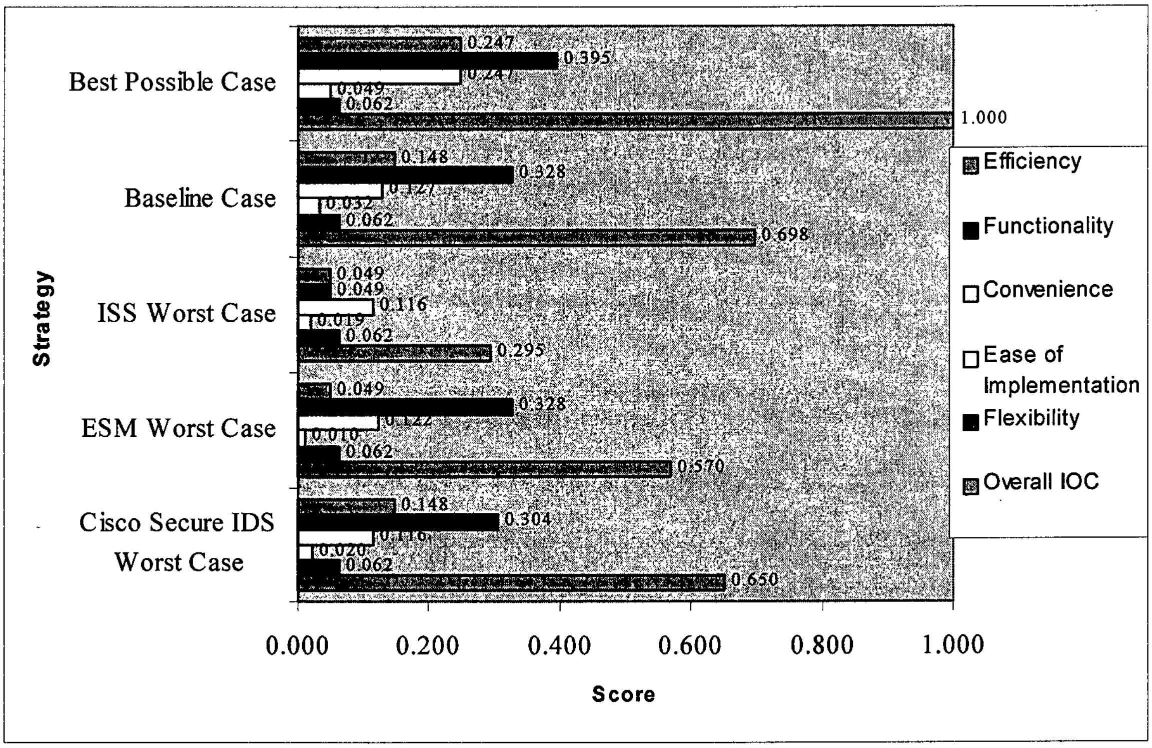


Figure 4-10: Alternative Comparisons with respect to IOC - Worst Case

ISS scores significantly lower in the IOC Worst Case conditions than ESM and Cisco Secure IDS, which implies there is a chance ISS could have a negative impact on system operational capability. The final hierarchy in the IAAM model, the Impact of Information Assurance on Resource Costs, is summarized as Table 4-19:

Table 4-19: Alternative Rankings and Scores with respect to IRC – Worst Case

Alternative	**Life Cycle Acquisition Costs (max = 0.40)**	**Personnel (max = 0.60)**	**Overall IRC Score (max = 1.00)**
Baseline	1 (0.333)	2 (0.092)	1 (0.425)
ISS Worst Case	tie – 3 (0.324)	3 (0.065)	3 (0.389)
ESM Worst Case	tie – 3 (0.324)	1 (0.097)	2 (0.421)
Cisco Secure IDS Worst Case	2 (0.327)	4 (0.061)	4 (0.388)

The Baseline Case edges ESM for the highest value in the IRC model, although as previously mentioned, differences this small may not be material. As a whole, the alternatives are grouped fairly tightly. This is due primarily because their collective low implementation and maintenance costs made the value 'Life Cycle Acquisition Costs' almost irrelevant to these alternatives. Figure 4-11 is a graphical representation of Table 4-19 presented above.

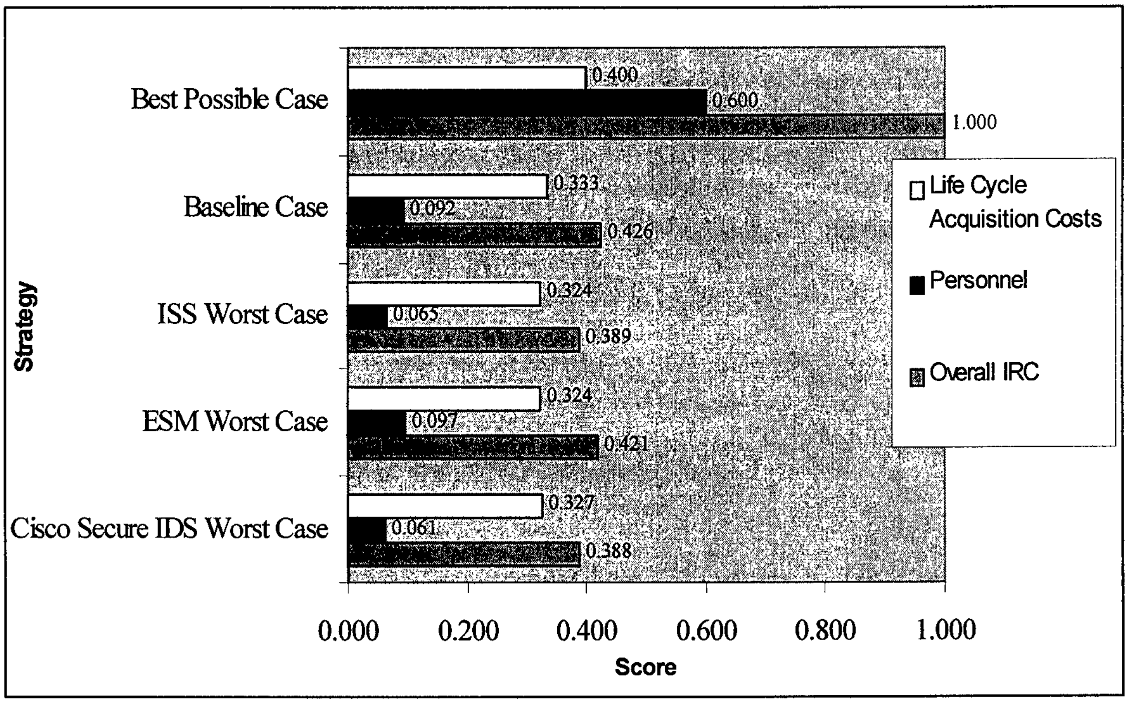


Figure 4-11: Alternative Comparisons with respect to IRC - Worst Case

Clearly, Figure 4-11 shows that the Personnel value gap still exists in the Worst Case conditions since all strategies still score very low in this measure. A maximum score of 0.600 may be earned in Personnel, however the highest ranked alternative in Personnel, ESM, scores only a 0.097.

Table 4-20 summarizes the Worst Case conditions alternative's respective rank within each hierarchy:

Table 4-20: Worst Case Conditions Alternative Rankings

Alternative	Information Assurance Rank	IOC Rank	IRC Rank
Baseline	4	1	1
ISS Most Likely	2	4	3
ESM Most Likely	3	3	2
Cisco Secure IDS Most Likely	1	2	3

Figure 4-12 shows each strategy's respective score in the IA, IOC, and IRC hierarchies for the Worst Case conditions. Notice that there is more variation in the IOC hierarchy than there was in the Most Likely Case due to the low score of ISS.

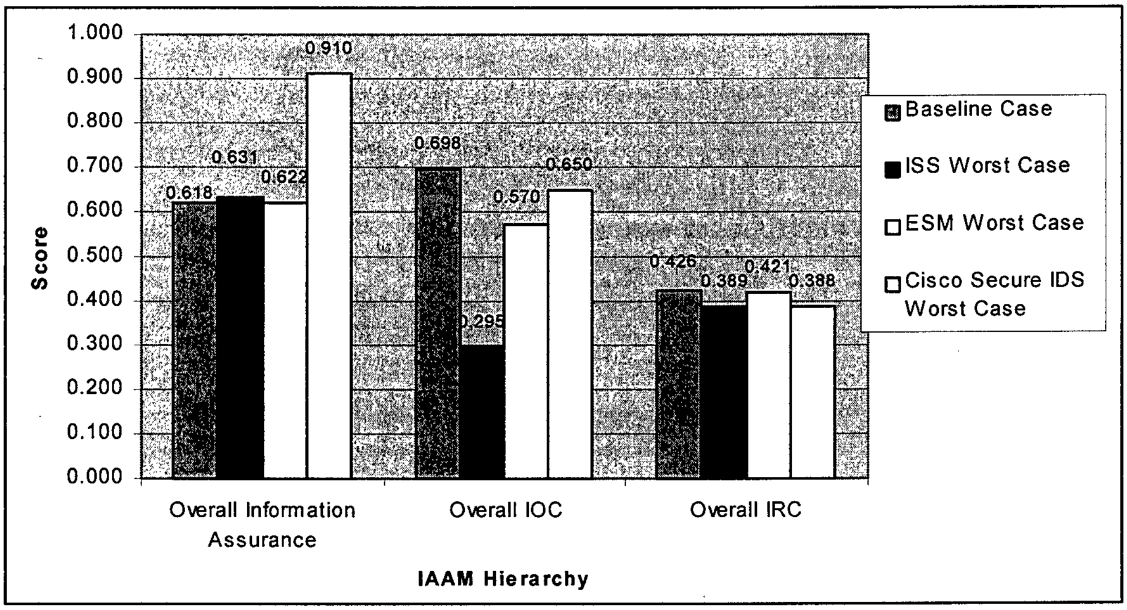


Figure 4-12: Worst Case Results, Separated by IAAM Hierarchy

The strategies separate in the IA and IOC hierarchies in the Worst Case conditions. Since Cisco Secure IDS had no variation with respect to IA in the Worst Case conditions, it kept its original score of 0.910. Cisco Secure IDS greatly outperformed the other strategies in the IA hierarchy Worst Case conditions since they all scored substantially lower than they did in the Most Likely Case. ISS has larger "downside" risk in the IOC hierarchy, implying that AFTAC personnel believe there is a possibility it could materially impact system operational capability if implementation were to go worse than expected.

4.6.2 Alternative Comparisons – Best Case

The Best Case conditions were scored to capture benefits of the strategy that were not initially considered or were uncertain to AFTAC personnel. Again, not all measures were believed to vary. Table 4-21 summarizes the Best Case conditions ranking for each alternative and the Baseline Case, which is unchanged:

Table 4-21: Alternative Rankings and Scores with respect to IA – Best Case

Alternative	**Information and IS Protection (max = 0.571)**	**Detection (max = 0.286)**	**Reaction (max = 0.143)**	**Overall Information Assurance Score (max = 1.00)**
Baseline	4 (0.333)	tie – 2 (0.199)	tie – 3 (0.086)	4 (0.618)
ISS Best Case	1 (0.560)	tie – 2 (0.199)	2 (0.098)	2 (0.857)
ESM Best Case	3 (0.465)	tie – 2 (0.199)	tie – 3 (0.086)	3 (0.750)
Cisco Secure IDS Best Case	2 (0.557)	1 (0.250)	1 (0.109)	1 (0.915)

The Cisco Secure IDS is again the highest ranked alternative within the Best Case conditions, scoring 91.5% of the total possible. While the relative improvement is small from Cisco Secure IDS's Most Likely score (a gain of 0.005), when added to the current AMIS configuration it nonetheless provides the best score on the Best Case conditions. In the Best Case, all alternatives separated themselves from the Baseline Case, improving their respective scores from the Most Likely Case. Figure 4-13 is a graphical representation of Table 4-21.

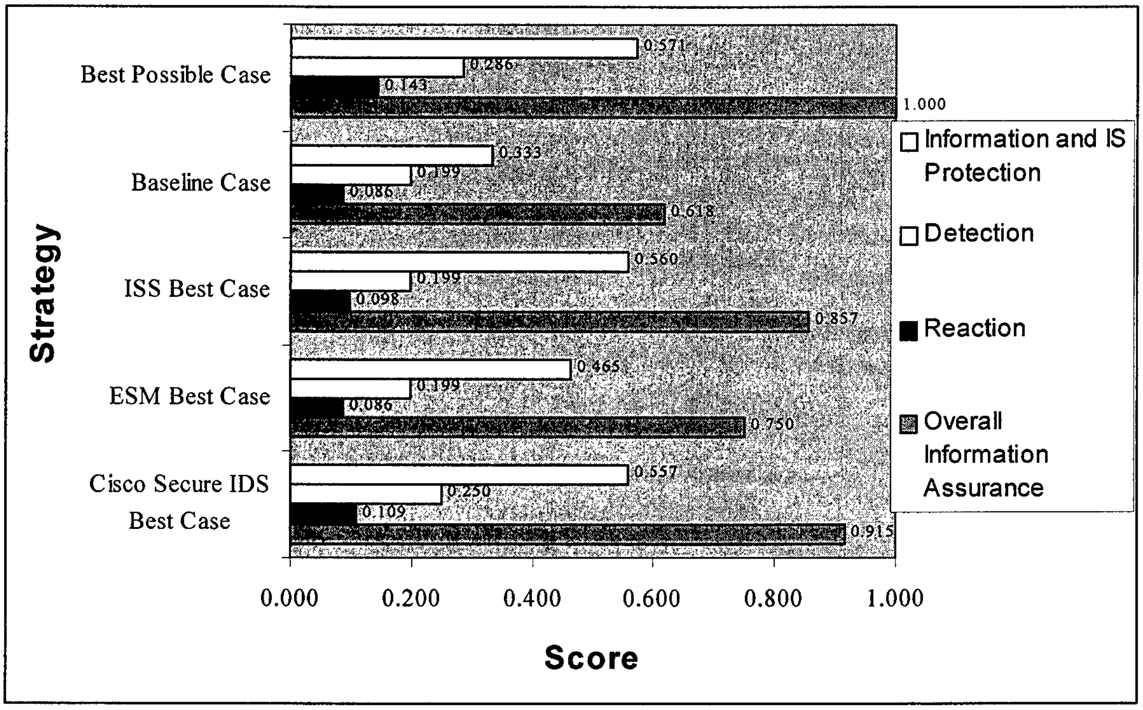


Figure 4-13: Alternative Comparisons with respect to Information Assurance - Best Case

In the Best Case, ISS actually performs better than Cisco Secure IDS in Information and IS Protection. This high score also propelled ISS to a high overall score, but still not high enough to overcome Cisco Secure IDS, which scored well throughout the hierarchy.

Table 4-22 details the rankings of the Best Case conditions alternatives with respect to the Impact of IA on System Operational Capability hierarchy:

Table 4-22: Alternative Rankings and Scores with respect to Impact of IOC – Best Case

Alternative	Efficiency (max = 0.247)	Functionality (max = 0.395)	Convenience (max = 0.247)	Ease of Implementation (max = 0.049)	Flexibility (max = 0.062)	Overall IOC Score (max = 1.00)
Baseline	tie – 1 (0.148)	3 (0.328)	tie – 1 (0.127)	1 (0.032)	tie – 1 (0.062)	2 (0.698)
ISS Best Case	4 (0.069)	2 (0.340)	tie – 3 (0.122)	tie – 3 (0.023)	tie – 1 (0.062)	4 (0.616)
ESM Best Case	tie – 1 (0.148)	1 (0.353)	tie – 1 (0.127)	2 (0.031)	tie – 1 (0.062)	1 (0.721)
Cisco Secure IDS Best Case	tie – 1 (0.148)	4 (0.304)	tie – 3 (0.122)	tie – 3 (0.023)	tie – 1 (0.062)	3 (0.658)

The ESM Best Case conditions actually improve system operational capability as it received a higher score than the Baseline Case. This is the only alternative and condition set within any of the analyses to actually improve IA and operational capability on the system. The Cisco Secure IDS, which was the clear winner in the IA hierarchy, ranks slightly behind the Baseline Case by only 0.04. A graphical representation is given in Figure 4-14.

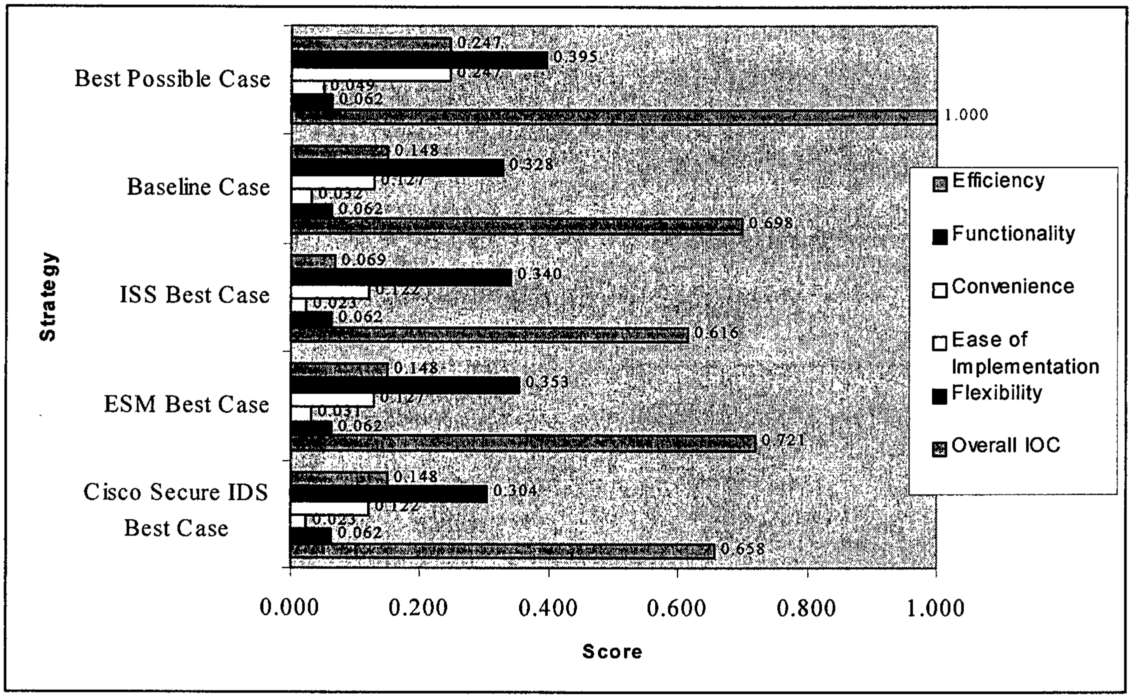


Figure 4-14: Alternative Comparisons with respect to IOC - Best Case

In the Best Case, ESM scores strongly in Functionality, which is the reason it ranks ahead of the Baseline Case in IOC. Cisco Secure IDS received the same scores for all values in the IOC hierarchy as did ESM, save Functionality. Cisco Secure IDS scored only a 0.304 in Functionality, a relatively low score compared to ESM and ISS. Table 4-23 shows the Best Case alternative rankings for the IRC hierarchy:

Table 4-23: Alternative Rankings and Scores with respect to IRC – Best Case

Alternative	Life Cycle Acquisition Costs (max = 0.40)	Personnel (max = 0.60)	Overall IRC Score (max = 1.00)
Baseline	1 (0.333)	2 (0.092)	2 (0.425)
ISS Best Case	2 (0.330)	3 (0.078)	3 (0.408)
ESM Best Case	3 (0.329)	1 (0.101)	1 (0.430)
Cisco Secure IDS Best Case	4 (0.327)	4 (0.064)	4 (0.391)

The ESM Best Case conditions again ranks higher than the Baseline Case with respect to the IRC hierarchy. Combined with the knowledge from the previous table, ESM Best Case can improve IA (although not the level of Cisco Secure IDS), increase operational capability, and consume less resource costs than the current system. It is important to note, however, that this is under Best Case conditions and should be considered as the upper limit of a strategy's potential. Figure 4-15 is a graphical representation of Table 4-23.

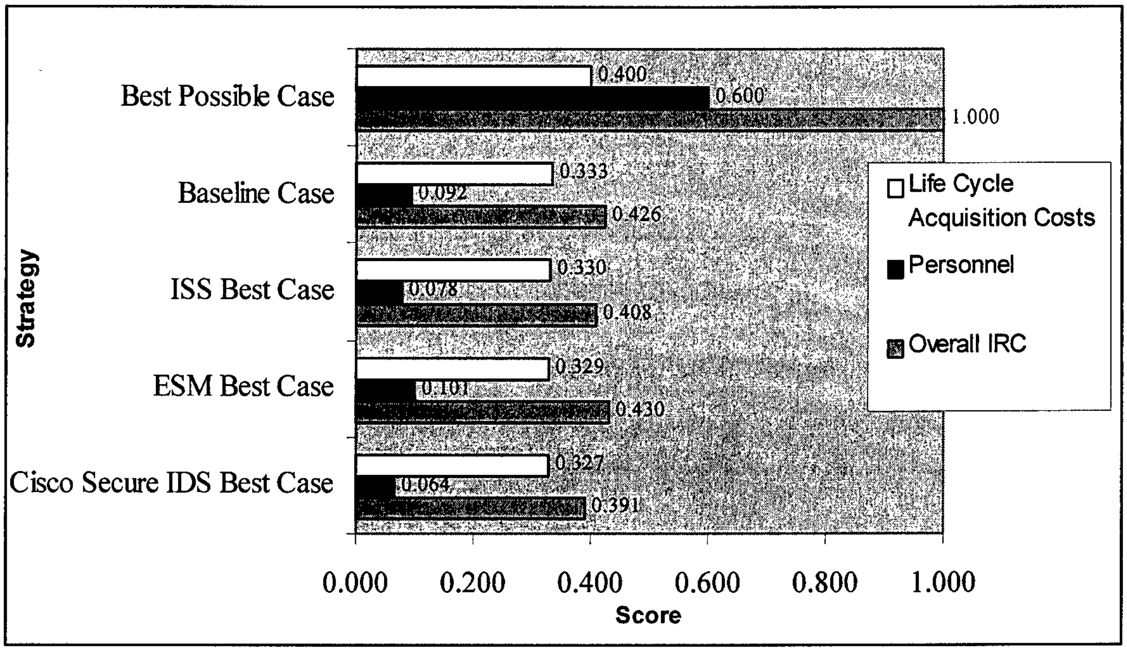


Figure 4-15: Alternative Comparisons with respect to IRC - Best Case

ESM scores higher than any other alternative in Personnel, causing it to be the highest ranked strategy in IRC for the Best Case conditions since there was little variation in the Life Cycle Acquisition Costs scores. It is important to note that even on Best Case conditions, a value gap in Personnel still exists. ESM's relatively high score of 0.101 in Personnel is still far from the best possible score of 0.600. Table 4-24 summarizes the alternatives' respective ranking within each hierarchy for the Best Case conditions. ESM dominated the Baseline Case on the Best Case conditions as it ranks higher in all three hierarchies.

Table 4-24: Summary of Best Case Alternative Rankings

Alternative	Information Assurance Rank	IOC Rank	IRC Rank
Baseline	4	2	2
ISS Most Likely	2	4	3
ESM Most Likely	3	1	1
Cisco Secure IDS Most Likely	1	3	4

Figure 4-16 shows the Best Case conditions results for each of the strategies. ISS, ESM, and Cisco Secure IDS all score substantially higher in the IA hierarchy. ESM scores higher than the Baseline Case in the IA, IOC, and IRC hierarchies, indicating that it provides increased information assurance, increased system operational capability, and will consume less AFTAC resources than the Baseline Case

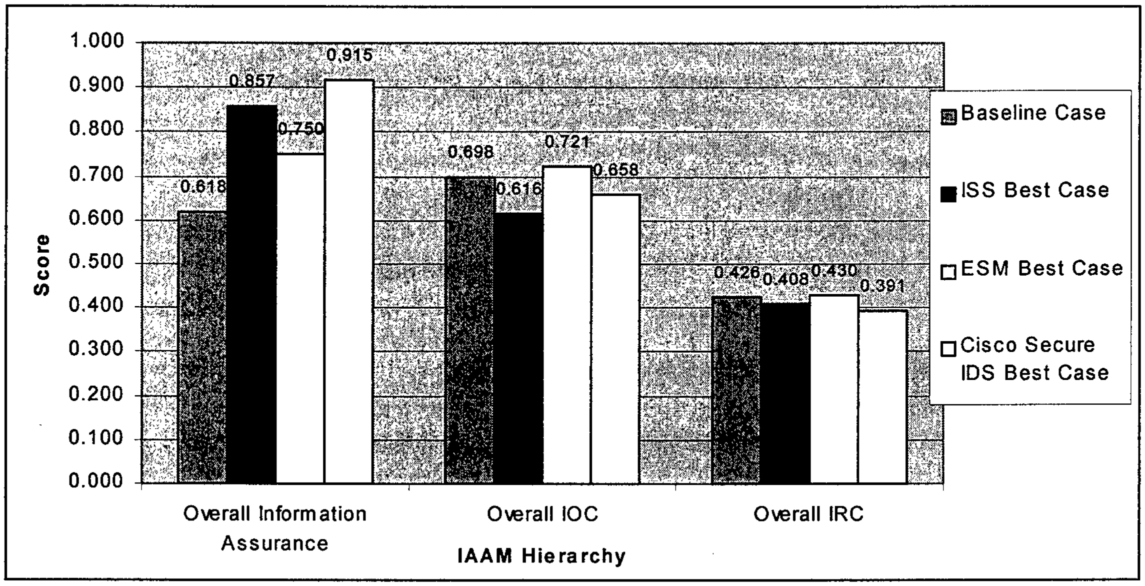


Figure 4-16: Best Case Results, Separated by IAAM Hierarchy

Figure 4-17, Figure 4-18, and Figure 4-19 show the range of each strategy with respect to the IA, IOC, and IRC hierarchies. Figure 4-17 shows that the Worst Case conditions for Cisco Secure IDS receives a higher score than the Best Case for all other alternatives. This implies that Cisco Secure IDS is clearly the best strategy with respect to the IA hierarchy alone, dominating all other alternatives.

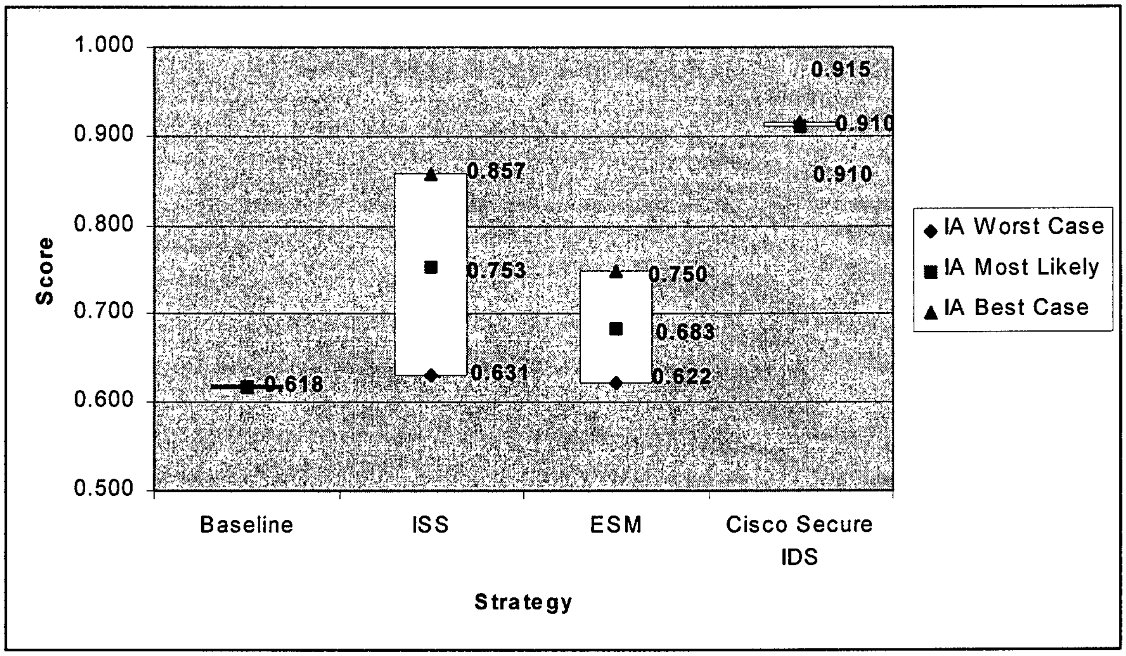


Figure 4-17: Strategy Range with respect to IA

Figure 4-18 depicts the Worst, Most Likely, and Best Case conditions for the IOC hierarchy. There is no single strategy that completely dominates the IOC hierarchy. For the Best Case conditions, ESM is the highest ranked alternative; however, for the Worst Case conditions it ranks below the Baseline Case and Cisco Secure IDS. ESM unfortunately has a wide range between its Best and Worst Case scores. ISS also exhibits a large range in the IOC hierarchy, indicating that there is uncertainty with this strategy's impact to system operational capability. Cisco Secure IDS exhibited the least variation in the IOC hierarchy, ranging from a Worst Case of 0.650 to a Best Case of 0.658. Although this is a decrease from the baseline IOC score of 0.689, Cisco Secure IDS does not appear to have a substantial "downside" risk.

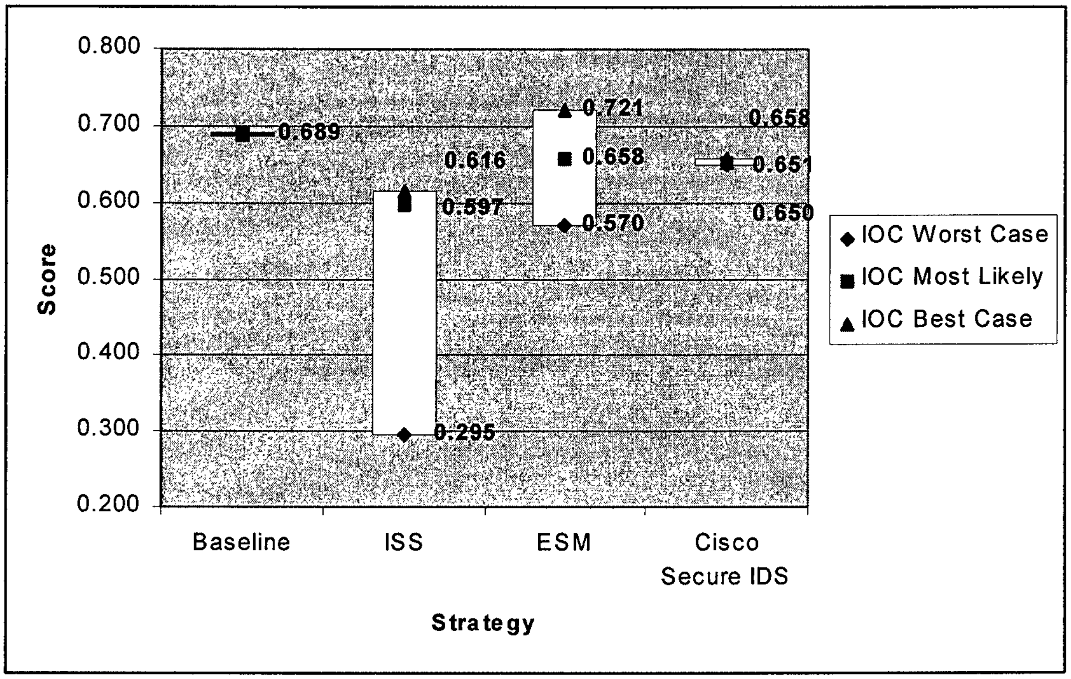


Figure 4-18: Strategy Range with respect to IOC

Figure 4-19 also shows that there is no guaranteed best alternative in the IRC hierarchy. While ESM Best Case edges the Baseline Case for the highest ranked alternative, it does not score higher in the Worst Case. ISS and Cisco Secure IDS are clearly the third and fourth ranked strategies with respect to IRC, however their ordering cannot be guaranteed due to having a slight overlap. Again, Cisco Secure IDS exhibited the least variation, however its Most Likely IRC score was lower than that of the Baseline Case, ISS, and ESM.

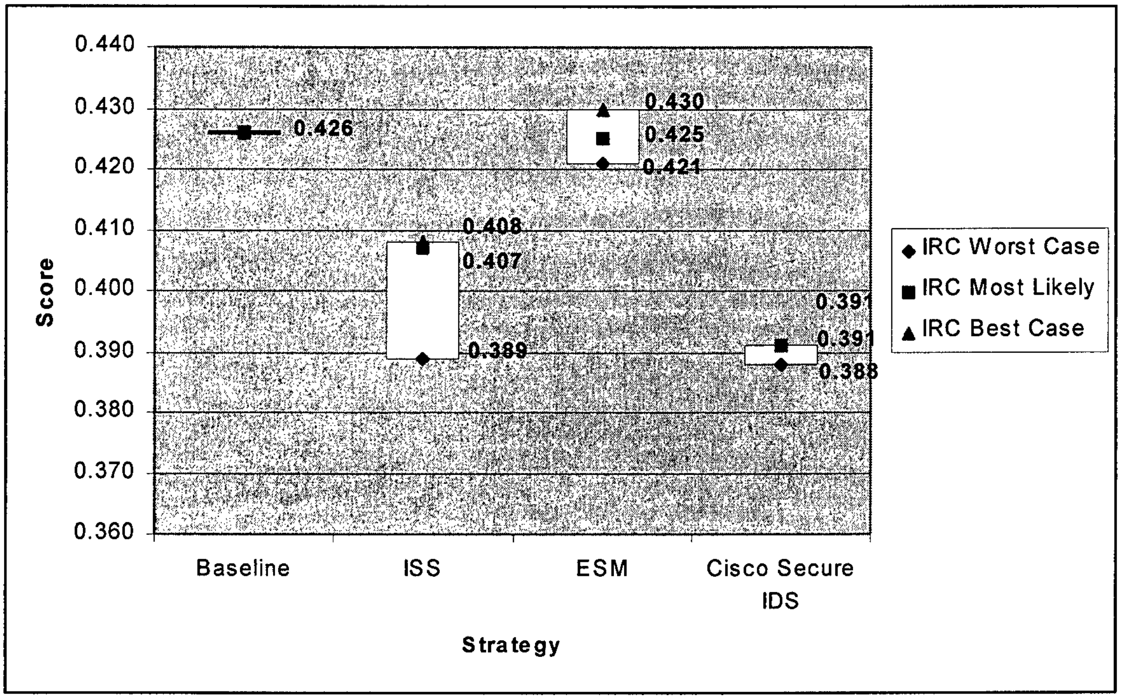


Figure 4-19: Strategy Range with respect to IRC

4.7 Weight Sensitivity Analysis

The total value for each alternative depends on the weights given to each measure; therefore a sensitivity analysis based on the weighting was performed to determine if and when the rank order of the alternatives changed. A sensitivity analysis on the weighting of the top-tier values for each of the three hierarchies for the Most Likely Case will be presented in this chapter. A sensitivity analysis on all other values and individual measures for the Best, Worst, and Most Likely Case was also performed but is not presented in this document. The vast majority of lower tier values were insensitive to weight changes at the local level.

One-way sensitivity analyses were performed for each value. The Microsoft Excel © spreadsheet used to generate the one-way sensitivity analysis in this report does have the ability to produce two or three-way sensitivity analysis should that be desired, although additional programming is required.

The sensitivity analysis will show if altering any weights would change the overall ranking of the alternatives in the given hierarchy. All sensitivity analyses are one-way, meaning that only one value at a time was varied independently. All other values at the same tier of the hierarchy kept their respective proportional weight ratios. For example, when performing a sensitivity analysis on the top tier values of the IA hierarchy, which are Information and IS Protection, Detection, and Reaction, only one value at a time was varied from 0.000 to 1.000 (at increments of 0.100) while the other two values held their original weight ratios. The local weights for Information and IS Protection originally were 4 / 7 (≅ 0.571), 2 / 7 (≅ 0.286), and 1 / 7 (≅ 0.143) respectively. As the weight for Information and IS Protection was varied, all three weights were still forced to sum to 1.000.

The formula used to determine the weights for the dependant values, Detection and Reaction, are given as Equation 4-1 and Equation 4-2 respectively, where w_p = Information and IS Protection weight, w_d = Detection weight, w_d^0 = Original Detection weight, w_r = Reaction weight, and w_r^0 = Original Reaction weight:

$$w_d = (1 - w_p) \text{ x } [w_d^0 / (w_d^0 + w_r^0)]$$

Equation 4-1: Formula to calculate Detection while varying Information and IS Protection [modified from Kirkwood, 1997: 82]

$$w_r = (1 - w_p) \text{ x } [w_r^0 / (w_r^0 + w_d^0)]$$

Equation 4-2: Formula to calculate Reaction while varying Information and IS Protection [modified from Kirkwood, 1997: 82]

Table 4-25 shows the respective weights for Information and IS Protection, Detection, and Reaction as Information and IS Protection is varied from 0.000 to 1.000 (original weights in bold):

Table 4-25: Weights as Information and IS Protection is varied from 0.000 to 1.000

Value	**Weight**											
Information and IS Protection	0.000	0.100	0.200	0.300	0.400	0.500	**0.571**	0.600	0.700	0.800	0.900	1.000
Detection	0.667	0.600	0.533	0.467	0.400	0.333	**0.286**	0.267	0.200	0.133	0.067	0.000
Reaction	0.333	0.300	0.267	0.233	0.200	0.167	**0.143**	0.133	0.100	0.067	0.033	0.000

Detection was then varied at increments of 0.100 holding Information and IS Protection and Reaction to their original comparative weight ratios. Table 4-26 presents the weights for Information and IS Protection, Detection, and Reaction as Detection was varied (original weights in bold):

Table 4-26: Weights as Detection is varied from 0.000 to 1.000

Value	**Weight**											
Detection	0.000	0.100	0.200	**0.286**	0.300	0.400	0.500	0.600	0.700	0.800	0.900	1.000
Information and IS Protection	0.800	0.720	0.640	**0.571**	0.560	0.480	0.400	0.320	0.240	0.160	0.080	0.000
Reaction	0.200	0.180	0.160	**0.143**	0.140	0.120	0.100	0.080	0.060	0.040	0.020	0.000

Finally, Reaction was varied in the same fashion as the previous two values; Table 4-27 gives their respective weights (original weights in bold):

Table 4-27: Weights as Reaction is varied from 0.000 to 1.000

Value	**Weight**											
Reaction	0.000	0.100	**0.143**	0.200	0.300	0.400	0.500	0.600	0.700	0.800	0.900	1.000
Information and IS Protection	0.667	0.600	**0.571**	0.533	0.467	0.400	0.333	0.267	0.200	0.133	0.067	0.000
Detection	0.333	0.300	**0.286**	0.267	0.233	0.200	0.167	0.133	0.100	0.067	0.033	0.000

The sensitivity analysis follows this procedure for all values within a hierarchical tier.

4.7.1 Information Assurance Sensitivity

AFTAC Experts originally gave Information and IS Protection a local weight of 4/7, or about 0.571. With this weight, Cisco Secure IDS was clearly the highest ranked strategy, receiving an IA score of 0.910. Figure 4-20 shows how the alternatives rank when the local weight for Information and IS Protection is varied between 0.0 and 1.0 in increment of 0.1. The vertical line shows the original local weight.

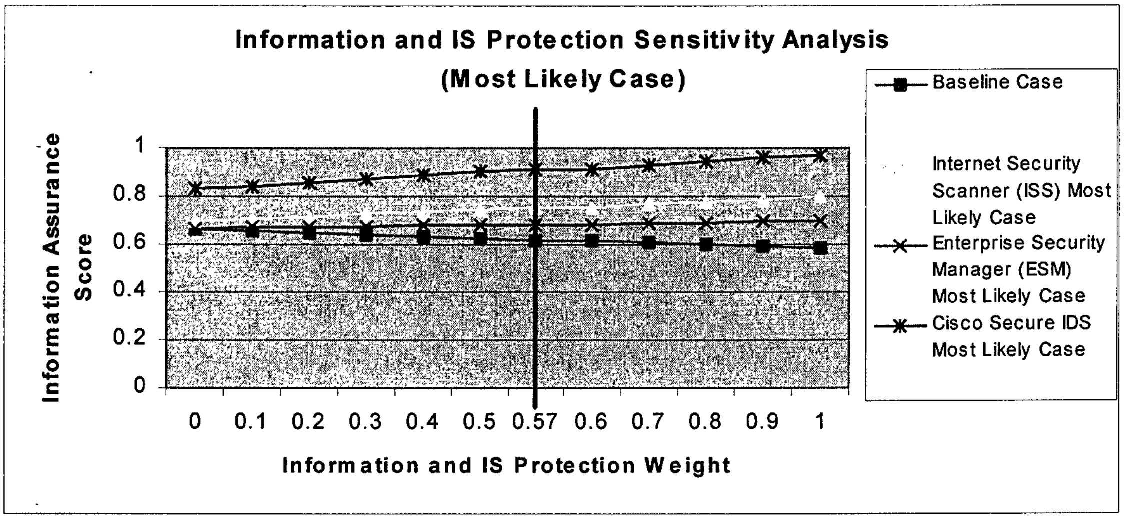


Figure 4-20: Information and IS Protection Sensitivity Analysis

Figure 4-20 shows that as Information and IS Protection's weight varies from 0.0 to 1.0, Cisco Secure IDS remains the highest ranked strategy for IA. The separation at an Information and IS Protection weight of 1.0 implies that Cisco Secure IDS scored extremely well in relation to this value.

Detection, which originally received a local weight of 2/7, or approximately 0.286, was also varied between 0.0 and 1.0 in increments of 0.1. Figure 4-21 presents the sensitivity analysis for Detection:

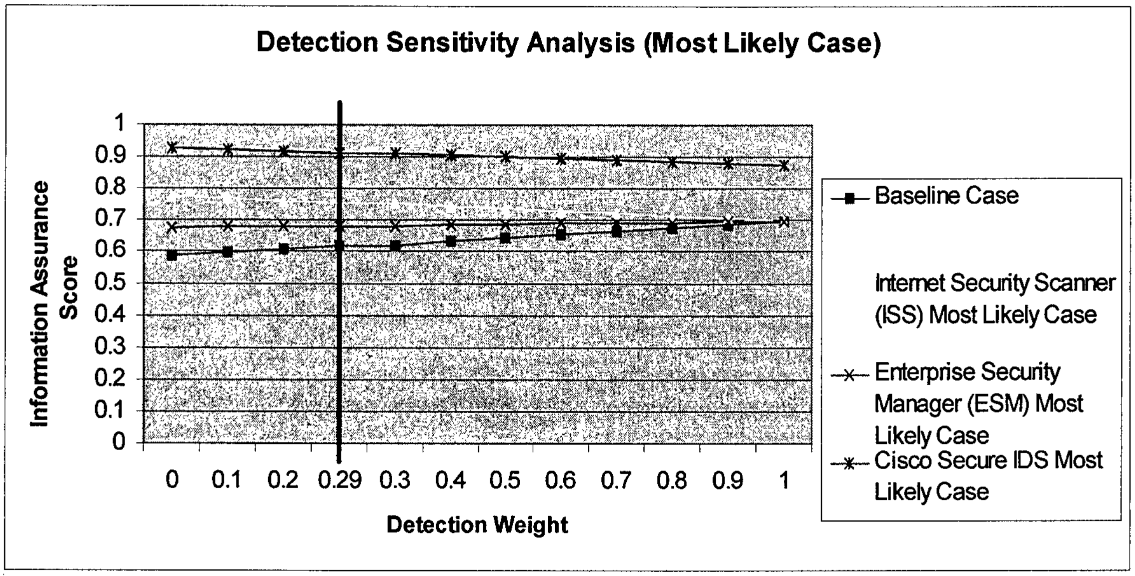


Figure 4-21: Detection Sensitivity Analysis

Again, Cisco Secure IDS is the highest ranked alternative across the entire weight spectrum. It is interesting to note that as Detection nears a local weight of 1.0, all other alternatives converge to the same overall IA score. This would imply that they all scored very similar in Detection measures.

Figure 4-22 shows the sensitivity analysis for Reaction, which originally received a local weight of 1/7, or about 0.143.

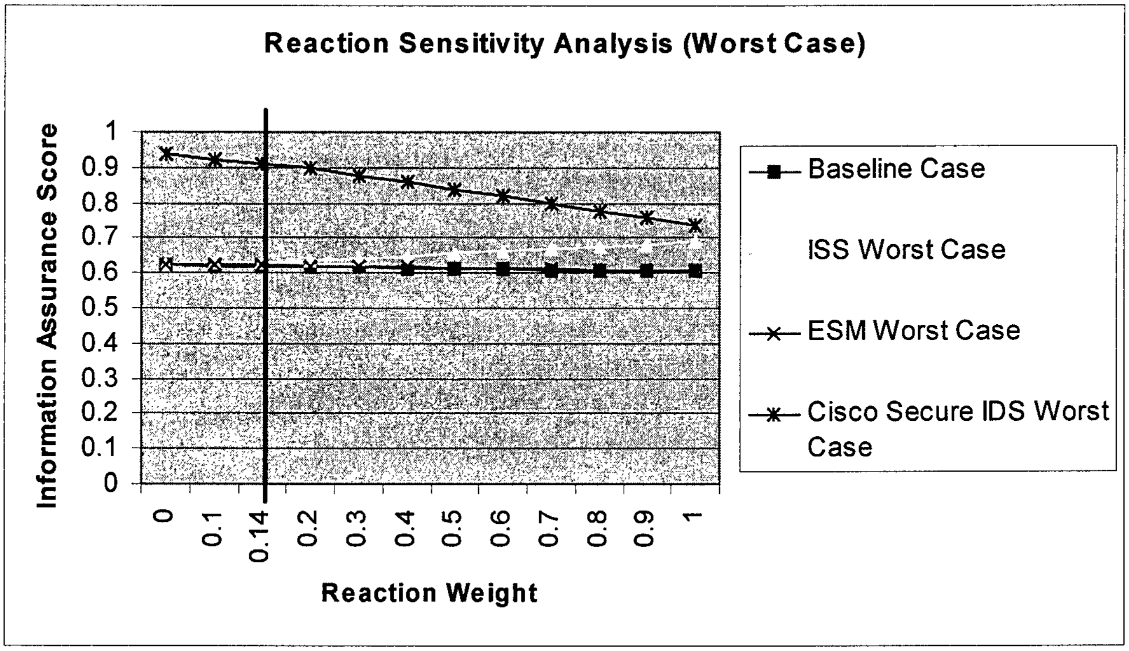


Figure 4-22: Reaction Sensitivity Analysis

Although the overall IA score for Cisco Secure IDS decreases as its local weight approaches 1.0, it still remains the highest ranked strategy. It is important to note that the difference between Cisco Secure IDS and ISS becomes very small if Reaction is weighted 1.0. Clearly, the ranking of these three alternatives is insensitive to the weighting of the IA hierarchy. At the top level of the IA hierarchy, the highest ranked strategy with the original weights, Cisco Secure IDS, remains the highest ranked strategy regardless of *any* Information and IS Protection, Detection, or Reaction weight.

4.7.2 Operational Capability Sensitivity Analysis

A sensitivity analysis on the top tier values in the IOC hierarchy was performed to determine if and where alternative changed rank order due to changing weights. Recall that Efficiency, Functionality, Convenience, Ease of Implementation, and Flexibility compose the top tier of the IOC model. The sensitivity analysis for Efficiency, which was originally weighted as 5/20.25 (about 0.247) is given in Figure 4-23:

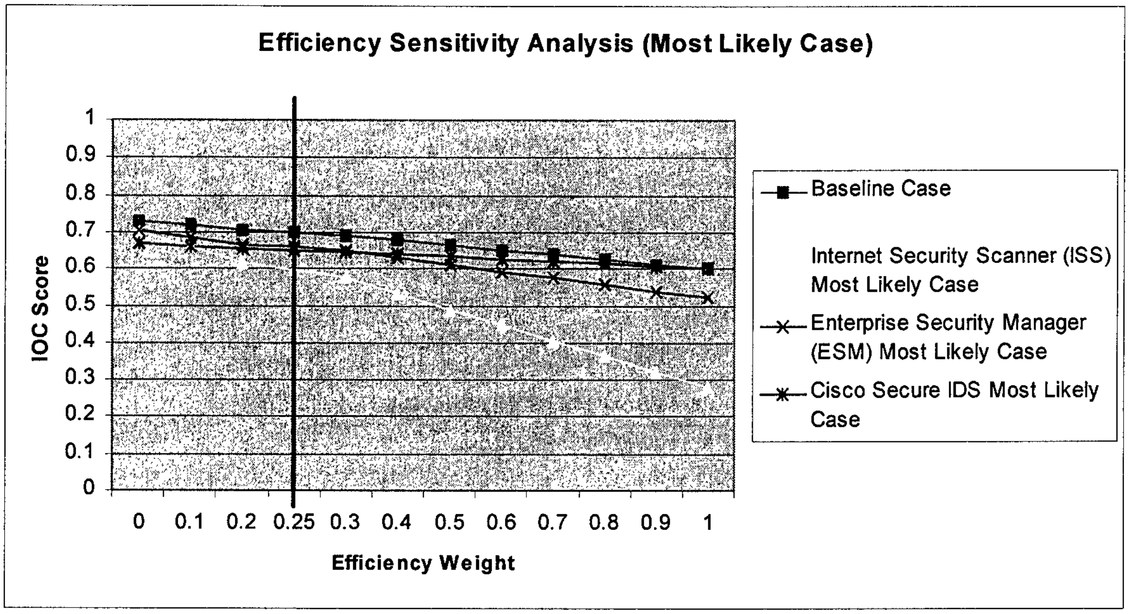


Figure 4-23: Efficiency Sensitivity Analysis

The Baseline Case, the current AMIS configuration, remains the highest ranked alternative in the IOC hierarchy until Efficiency receives a weight of 1.0, where it then meets with Cisco Secure IDS. Notice the rapid decline of the ISS strategy, implying that it scored low in Efficiency and as Efficiency becomes more important, the strategy does quite poorly.

AFTAC experts originally weighted Functionality at 8/20.25, or 0.395. The sensitivity analysis for Functionality is shown in Figure 4-24:

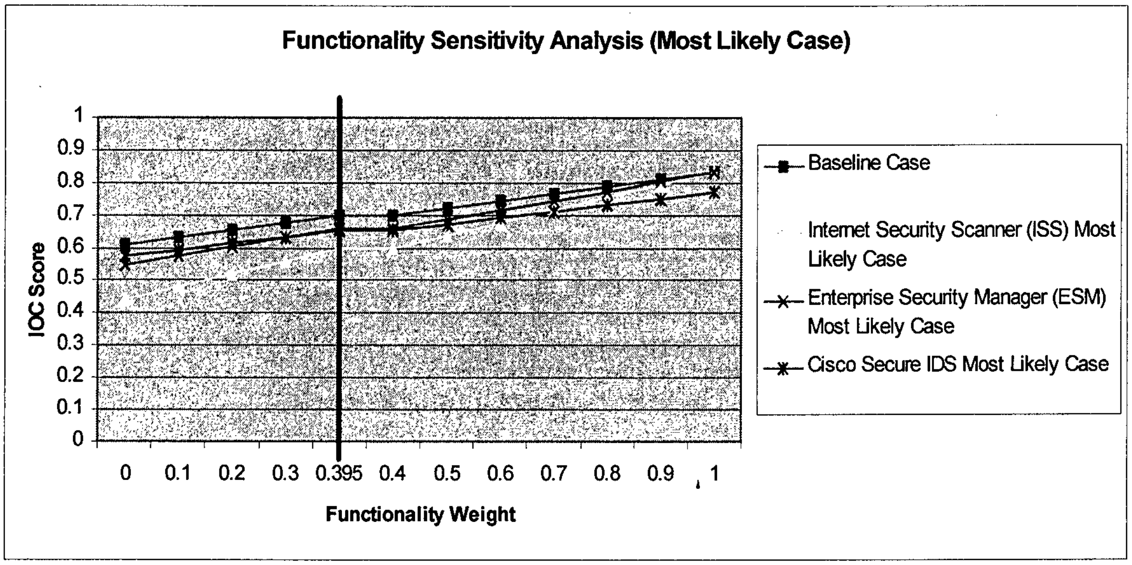


Figure 4-24: Functionality Sensitivity Analysis

The Baseline Case is the highest ranked alternative until Functionality reaches a weight of 0.9, where it then converges with ISS and ESM. The Cisco Secure IDS was the second best alternative when Functionality was weighted below 0.2, but was overtaken by ESM afterwards and eventually became the lowest ranked strategy.

Convenience originally received a weight of 5/20.25, or approximately 0.247. Figure 4-25 displays the sensitivity analysis for Convenience as it varied form a weight of 0.0 to 1.0:

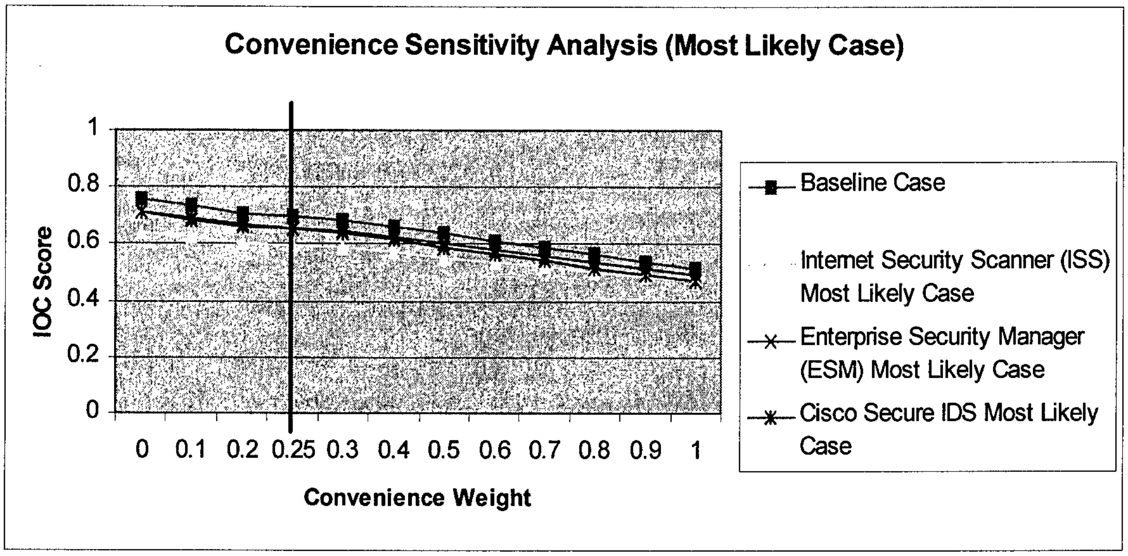


Figure 4-25: Convenience Sensitivity Analysis

All strategies remain close to each other throughout the weight spectrum, converging tightly when Convenience is weighted a 1.0. The Baseline Case does remain the highest ranked alternative throughout.

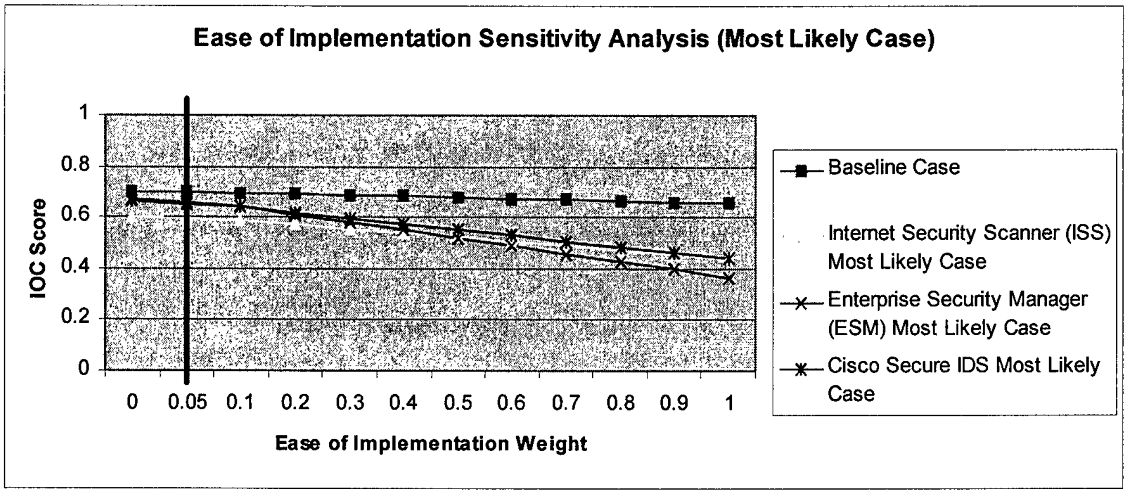


Figure 4-26: Ease of Implementation Sensitivity Analysis

Figure 4-26 presents the sensitivity analysis for Ease of Implementation, which originally received a weight of 1/20.25, or 0.049. The Baseline Case remains the best in Ease of Implementation, which makes intuitive sense since it is already implemented.

Therefore, as the weight for Ease of Implementation approaches 1.0, it separates itself even further from the rest of the strategies. Depending on the exact weight of Ease of Implementation, the rank order of ISS, ESM, and Cisco Secure IDS switch, with each being the second, third or fourth ranked alternative. From a weight of 0.0-0.2, ESM and Cisco are ranked ahead of ISS. At 0.2, Cisco's score decreases faster than ESM's, leaving ESM the highest ranked strategy until it converges with ISS at 0.7.

Flexibility originally received a weight of 1.25/20.25 (about 0.062) in the IOC hierarchy. Figure 4-27 shows the sensitivity for Flexibility as its weight is varied from 0.0 to 1.0:

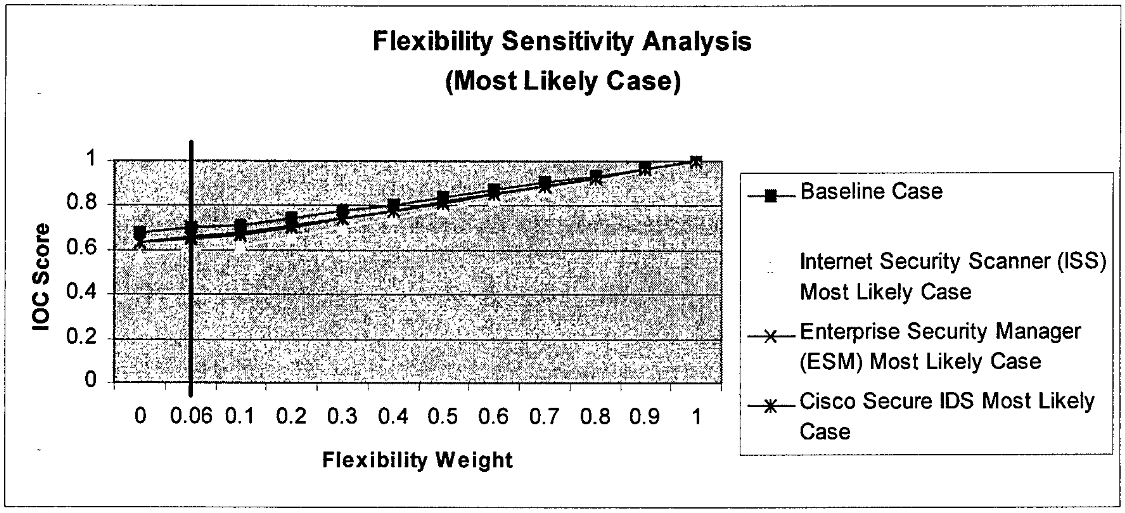


Figure 4-27: Flexibility Sensitivity Analysis

Every strategy received a perfect score for Flexibility since all were determined to be Upgradeable and Expandable. Therefore, if Flexibility were to have a weight of 1.0, all alternatives would receive a perfect IOC score, which is exactly what Figure 4-27 illustrates.

4.7.3 Impact of IA on Resource Costs Sensitivity Analysis

The IRC hierarchy had two values in its top tier: Life Cycle Acquisition Costs and Personnel. As with the other hierarchies, each of these was varied between 0.0 and 1.0 in increments of 0.1 in order to determine if any alternative rankings change depending on their respective weights. Again, recall that this analysis can be performed at any tier of the hierarchy.

Figure 4-28 displays the sensitivity analysis for Life Cycle Acquisition Costs, which was originally weighted as 0.4:

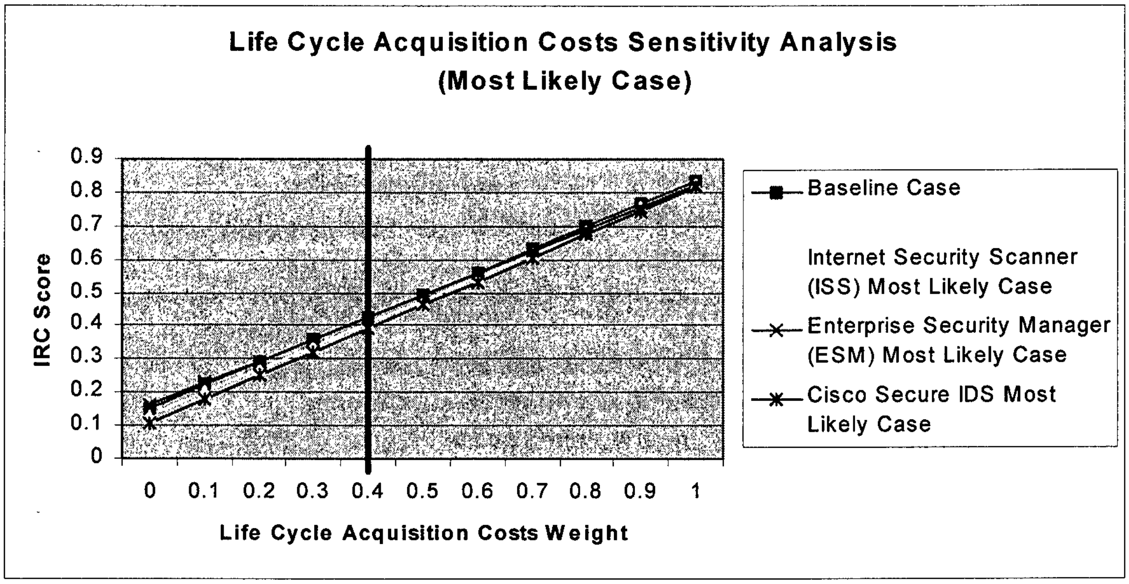


Figure 4-28: Life Cycle Acquisition Costs Sensitivity Analysis

Since all alternatives are relatively inexpensive to AFTAC, the strategies are insensitive. The Baseline Case is the least expensive and is slightly better than the other three alternatives throughout the hierarchy. An alternative that was very expensive to install and maintain would have had a much flatter slope on the graph than the current alternatives. The reason that the slope is so steep in Figure 4-28 is due to the weaker performance of all the alternatives in Personnel.

AFTAC experts weighted Personnel at 0.6 since they determined it was somewhat more valuable than dollar cost. Figure 4-29 shows the sensitivity analysis for Personnel:

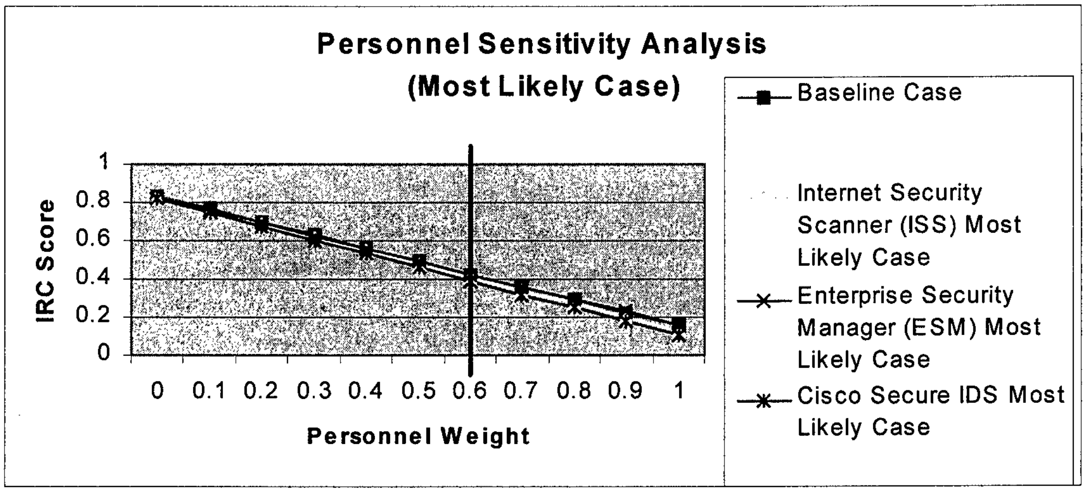


Figure 4-29: Personnel Sensitivity Analysis

Again, all strategies scored approximately the same, which produces little sensitivity to weighting. The steep negative slope for each alternative shows that all scored equally low in 'Personnel.' When its weight approaches 1.0, meaning it is the sole measure for the IRC hierarchy, the value produced to AFTAC is minimal.

Given the small number of alternatives analyzed, it is not surprising that they were relatively insensitive to the weighting, especially in the IA and IRC hierarchies. The IOC hierarchy had five top tier values, with very different original weights, and therefore was more sensitive to major weight changes than the IA or IRD hierarchy. As was stated earlier, this weight insensitivity occurred throughout the hierarchy.

4.8 Conclusions

The Information Assurance Analysis Model, developed in cooperation with experts from the Air Force Technical Applications Center, was used to analyze the current level of IA and the impact three different alternatives could have on an operational system. The alternatives were analyzed as the Most Likely Case, the Worst Case, and the Best Case since AFTAC personnel were asked to make predictions on their performance and could not give an accurate point estimate for some measures. A sensitivity analysis was then conducted to show how the alternatives would have ranked had personnel weighted values differently. This illustrative analysis demonstrates the type of insight that the decision-makers at AFTAC can gain when utilizing the IAAM to evaluate information assurance alternatives. A robust set of measures and analyses were presented to demonstrate the range of support that can be provided to the decision-maker. IAAM cannot only calibrate the current level of information assurance, it can also aid in the analysis of IA alternatives.

Chapter 5 is a summary of the project and will discuss such topics as lessons learned, opportunities for future work, and general impressions drawn from the project.

5. Project Conclusions

The objective of this thesis project was to provide a Department of Defense organization with a quantitative tool to measure and improve their level of information assurance. The Information Assurance Analysis Model (IAAM), composed of the Information Assurance (IA), Impact of IA on System Operational Capability (IOC), and Impact of IA on Resource Costs (IRC) value hierarchies, was created in order to meet the stated objective. Built in cooperation with AFTAC information assurance and information systems experts, the IAAM represents information assurance needs both specific to AFTAC (represented in the hierarchy weights), and to the DoD as a whole (represented in hierarchy values). The model provides decision-makers with the insight to aid in making the difficult and complex decisions regarding the delicate balance between information assurance, system operational capability, and resource costs.

5.1 Summary of Previous Chapters

The first Chapter of this thesis discussed the beginnings of the Internet and the inherent risks associated with it. The freedom of open communication afforded by the Internet revolutionized the speed in which decision-makers could gather, process, and disseminate information. However, the Internet was not originally designed to serve the world's population and security problems arose almost immediately after its creation. Today, the United States and its military depend heavily on interconnected information systems for their everyday operations and therefore need to insure the information contained is protected. Information assurance is critical to the safety and well being of

America, for one well planned and executed attack on a sensitive U. S. information system could cause catastrophic results.

A literature review detailing the Department of Defense's (DoD) position on information assurance was presented in the beginning of Chapter 2 to illustrate the importance it plays in today's military environment. Literature detailing civilian sector IA concerns was also discussed to show that information assurance must be a community wide effort. Although both the military and civilian sectors pronounced the need for solid information assurance strategies, to date there have been few attempts to measure it available in the public literature. It was then determined that Value Focused Thinking (VFT) provided a solid theoretical framework for the problem of measuring information assurance. Chapter 2 concluded with a review of the earlier efforts to model information assurance with VFT, none of which had been operationally tested. This thesis built upon the knowledge of DoD doctrine, information assurance literature, and past IA models to develop, in cooperation with the Air Force Technical Applications Center (AFTAC), an operational Information Assurance Analysis Model (IAAM) that would be tested on their AFTAC Mission Information System (AMIS).

Working with information assurance experts at AFTAC, it was verified that the IAAM should contain three separate hierarchies: Information Assurance, the Impact of Information Assurance on System Operational Capability, and the Impact of Information Assurance on Resource Costs. The development of these three hierarchies using the VFT process, which included creating values and their associated measures and weights, was reviewed in Chapter 3 and presented in detail in the Appendix. The contributions of

AFTAC personnel above and beyond their required duty allowed this project to become a reality. They cannot be given enough thanks for their time and effort.

AFTAC personnel proposed three separate information assurance strategies that they were considering for implementation into AMIS. These alternatives, along with the current AMIS system, were analyzed using the model. The result of this study, along with a sensitivity analysis on the value weights, is presented as Chapter 4.

The Appendix is a detailed review of the hierarchies, to include value definitions and rationale, as well as measure functions. Additionally, a Microsoft Excel © spreadsheet tool was created to help analyze the model and its results. The spreadsheet has the ability to insert and delete measures as deemed necessary to accommodate evolving assurance requirements and needs.

5.2 Project Objectives

As stated, the goal of this thesis was to provide a model that could be used by military or civilian organizations to help improve their information assurance. However, the model must be focused to capture specific necessities of the organization using it. Therefore, the IAAM was created with the intention that it could be used by a variety of organizations by building in the capability to be fined-tuned to fit each specific organization's unique needs.

Ultimately, the IAAM should be able to be used without VFT expert assistance; nevertheless, if the model is used incorrectly, it could lead to mistakes and thus the utmost care should be made when using the model to make decisions. The IAAM as it currently exists should therefore be used in cooperation with a VFT expert. It should be noted, however, the AFTAC personnel who participated in the model development exhibited a great deal of understanding of VFT as the project progressed.

The IAAM met the project objectives for both the AFIT and the AFTAC focus. Senior leadership at AFTAC have expressed an interest in implementing the IAAM into their information assurance decision-making process.

5.3 Future Research

Information assurance will remain a problem as long as people desire another's information. Therefore, this work must continue to evolve with computer technology it is designed to protect. While the values for this model are likely to remain for a period of time, it is unlikely that *any* assurance model that remains static will remain effective. Technology evolves quickly; what is great today will only be good tomorrow, and what is good today may be useless tomorrow. The IAAM model was designed to be an operational information analysis tool. Emphasis was placed on creating a model that would provide insight to decision-makers. Future research should therefore continue to focus on improving the insight gained from using this tool.

It would be advantageous to apply this model to other systems at AFTAC that are of a higher classification to see which adjustments might be required. Again, this model does not necessarily have to remain in its present form to be beneficial to an organization. Weighting does provide the flexibility to re-focus the model. However, if a uniquely different system does require adjustments beyond mere re-weighting, the existing hierarchies and measures provide a starting framework for future efforts.

This model did try to capture some uncertainty by analyzing the Most Likely, Worst, and Best Case conditions for the alternatives. However, a probabilistic risk assessment was not incorporated beyond the Best and Worst Case conditions mentioned. Utility theory accounts for decision-maker risk tolerance by assessing the probability of different events occurring, and if used properly will provide the decision-maker with a tool specifically tailored to that person's preferences. The incorporation of risk is clearly an additional possibility.

As personnel become more familiar with the IAAM and its uses, it can be utilized in conjunction with other analysis techniques. A further extension might be constructing an optimization to select the correct portfolios maximizing the fundamental value score. A linear program used in conjunction with VFT principles would combine the two techniques to provide a model with even greater precision. For example, personnel could use VFT to generate value hierarchies representing what was important the organization's information assurance as was done in this thesis. The linear program would then multiply the value coefficient by the alternative's score, producing an overall information assurance total.

5.4 Conclusions

The Information Assurance Analysis Model is one step towards solving the information assurance dilemma. Decision-makers will continue to struggle to achieve a balance between information assurance, system operational capability, and resource costs. The work presented in this thesis provides organizations with a quantitative tool to help find the balance between these competing values in order to improve their mission effectiveness.

Appendix. Value Hierarchies and Associated Measure Functions

The objective of this project was to develop a model to measure and improve Information Assurance (IA) at AFTAC using the process of Value Focused Thinking (VFT). The system chosen for study was the AFTAC Mission Information System (AMIS). AMIS carries a SECRET classification, therefore it stores and processes valuable information that requires protection. Joint Doctrine defines Information Assurance to be:

> Information Operations (IO) that protect and defend information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities [JP 3-13, 1998: I-9].

Improving IA may impact the System Operational Capability (IOC) and AFTAC Resource Costs (IRC); consequently these considerations must also be included in the model. Figure A-1 shows the relationship between IA, IOC, and IRC. A best case scenario would be one that increases information assurance, positively impacts system operational capability, and implements the changes at a low cost to AFTAC.

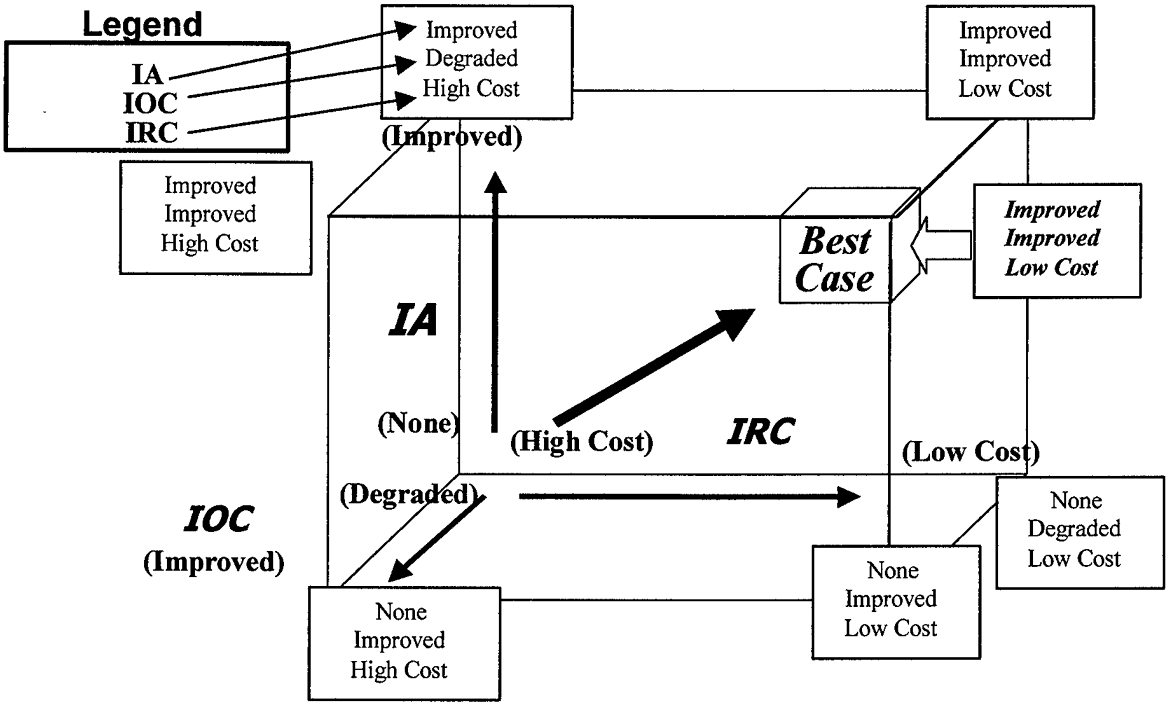


Figure A-1: Relationship between Information Assurance (IA), Impact of IA on System Operational Capability (IOC), and Impact of IA on Resource Costs (IRC) [modified from Hamill, 2000: 4-2]

In order to capture the three key factors, the Information Assurance Analysis Model (IAAM) has been constructed as shown in Figure A-2. There are three main hierarchies in the model: Information Assurance (IA), Impact of IA on System Operational Capability (IOC), and Impact of IA on Resource Costs (IRC).

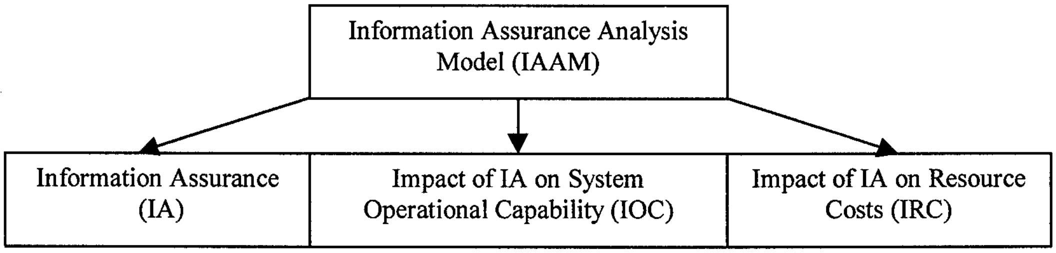

Information Assurance Analysis Model (IAAM)
Information Assurance (IA)
Impact of IA on System Operational Capability (IOC)
Impact of IA on Resource Costs (IRC)

Figure A-2: The Information Assurance Analysis Model

The three hierarchies are used to find a balance between these competing factors in order to provide the best balance of assurance and system capability at the lowest cost. The current level of IA at AFTAC was baselined in order to provide a frame of reference for this study. This allowed value gaps, defined to be areas where improvement can be gained, to be identified on AMIS. Several different IA strategies were then proposed, scored, and rank ordered using the model. Combined, this information provided valuable insight that AFTAC decision-makers can use to determine which IA strategies should be selected for implementation.

The Information Assurance (IA) hierarchy is first discussed, followed by the Impact of IA on System Operational Capability (IOC) hierarchy, and finally the Impact of IA on Resource Costs (IRC) hierarchy. The IA hierarchy contains values associated with measuring what AFTAC personnel determined to be important regarding the information assurance on AMIS. The IOC hierarchy measures the change in operational capability an IA strategy is projected to have upon the system, not the actual system operational capability. Likewise, the IRC hierarchy measures the impact an IA strategy will have on AFTAC resource costs, and is not a measure of AFTAC's overall resources.

Information Assurance

The first step in the VFT process is to identify what values system experts feel are important to each of the three hierarchies. Beginning with the IA hierarchy, a definition of each value, the rationale behind it, and an explanation of the single dimensional value functions used to measure the value will be presented. The full IA hierarchy is shown as Figure A-3:

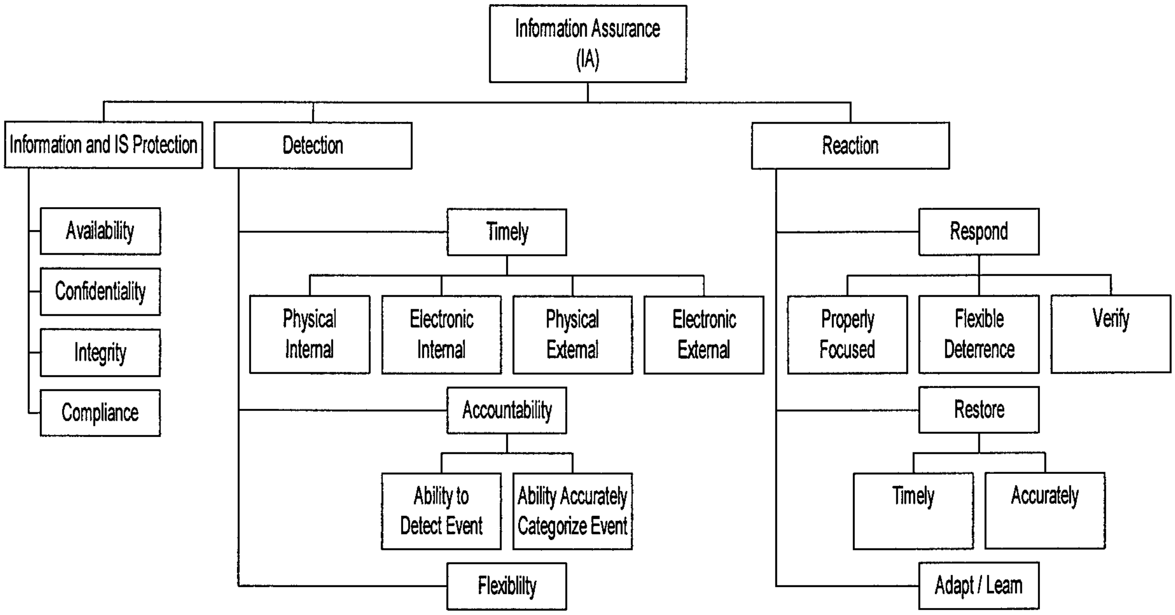


Figure A-3: Information Assurance (IA) Value Hierarchy

The IA hierarchy is separated into three main sub-hierarchies: Information and Information Systems (IS) Protection, Detection, and Reaction. These values were taken from the *JP 3-13* definition of IA given on the first page of this document. When presented to AFTAC information assurance specialists, they concurred that an IA value hierarchy must capture all the elements of protection, detection, and reaction in order to be a complete model. It is important to note that information assurance is not a synonym for computer security; IA is the entire process of defending valuable information.

Information and Information Systems (IS) Protection will be discussed first followed by Detection and Reaction. The value hierarchy is a representation of AFTAC values and should not to be read as a flow chart. Like an organizational chart, the ordering of the values at any given level is not significant. The hierarchy could read Reaction, Detection, and Protection from left to right and not disturb the model. The weights placed on each value, which are discussed in Chapter 3, signify the importance of that particular value.

Information and Information Systems (IS) Protection

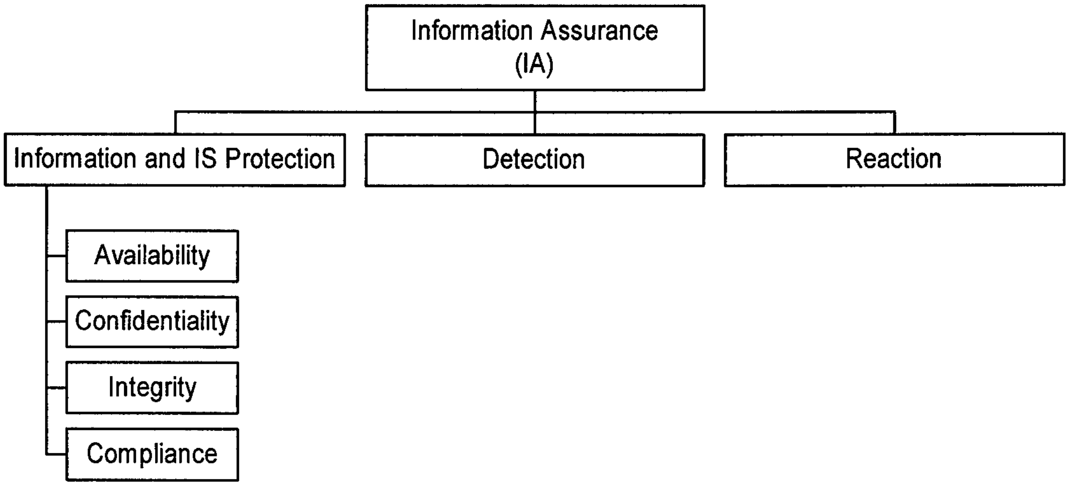


Figure A-4: Information and Information Systems (IS) Protection

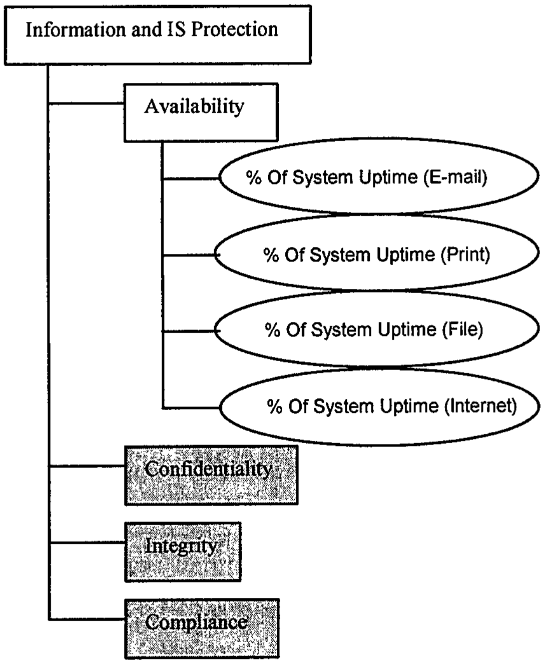
Information and Information Systems (IS) Protection: Measures taken to protect information and information systems. An event is defined as any abnormal activity that occurs to the system that could compromise information. Malicious attacks by terrorists or an AFTAC employee accidentally accessing restricted information are both considered events.

Rationale: Protection is a key consideration of any IA strategy. It includes both electronic protection, physical security measures, and policies that prevent unauthorized personnel from accessing information. Protection is critical because it is responsible for preventing events before they ever occur; it is impossible for a foe to corrupt information if unauthorized access cannot be attained. It is important to note that protection, in this hierarchy, includes both information and information systems; therefore protection against both electronic and physical attacks are considered.

Information and IS Protection is a very broad term requiring further definition. Using both joint doctrine and AFTAC experts, Information and IS Protection was separated into Availability, Confidentiality, Integrity, and Compliance. The discussion begins with the uppermost value in the hierarchy and progresses downward until all values are covered; this pattern is followed throughout the appendix. Recall that the position of a value within any individual tier does not reflect its level of importance.

Availability: The system is available to authorized personnel when needed.

Rationale: Availability is important because authorized users and system administrators must be able to utilize the system in order to perform their missions. Availability is a product of good protection; a properly protected system will be available to authorized personnel when they need it.


Information and IS Protection
Availability
% Of System Uptime (E-mail)
% Of System Uptime (Print)
% Of System Uptime (File)
% Of System Uptime (Internet)
Confidentiality
Integrity
Compliance

Measure: Availability is measured as the percentage of system uptime for both users and support personnel. Since the system may perform more than one function, and these functions may be available independently from one another (for example, e-mail may be available when the print server is not) there are separate measures for each critical system function. AMIS, the system under study, has four primary services (e-mail, print, file, and Internet); therefore there are four separate value functions. Each service was weighted separately, reflecting the different levels of importance between the services. Taken independently, AFTAC values each of the services in the same pattern, so the shape of the value function is constant for all four system functions. The graphs in Figure A-5 through Figure A-8 show that no value is given until the servers are available for at least 80% of the time. Anything below this 80% Availability point is unacceptable to the organization. There is a sharp rise in value from 90% to 95% availability because the agency feels that anything less than 95% availability would severely hamper mission capabilities.

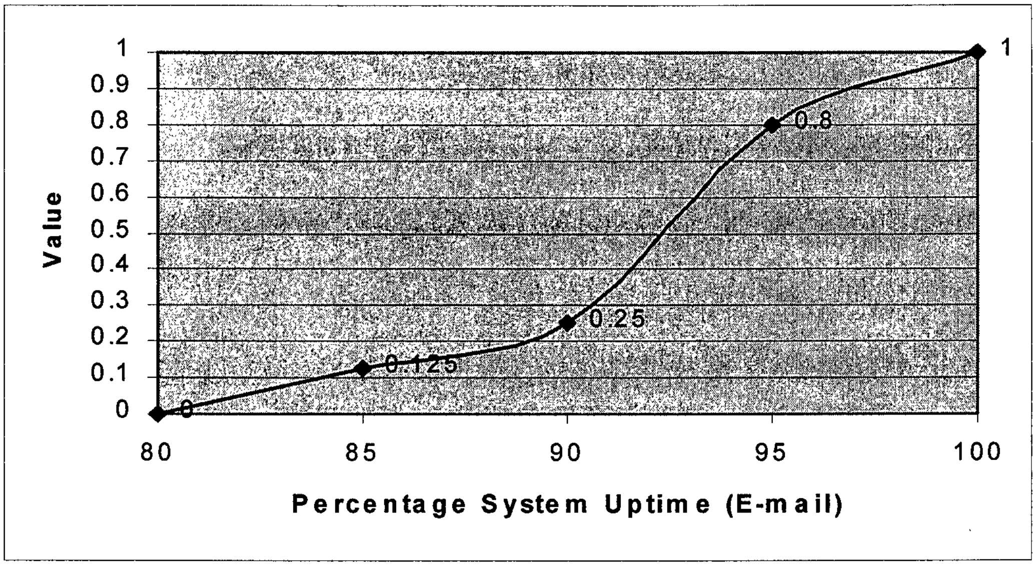


Figure A-5: Percentage of System Uptime (E-mail)

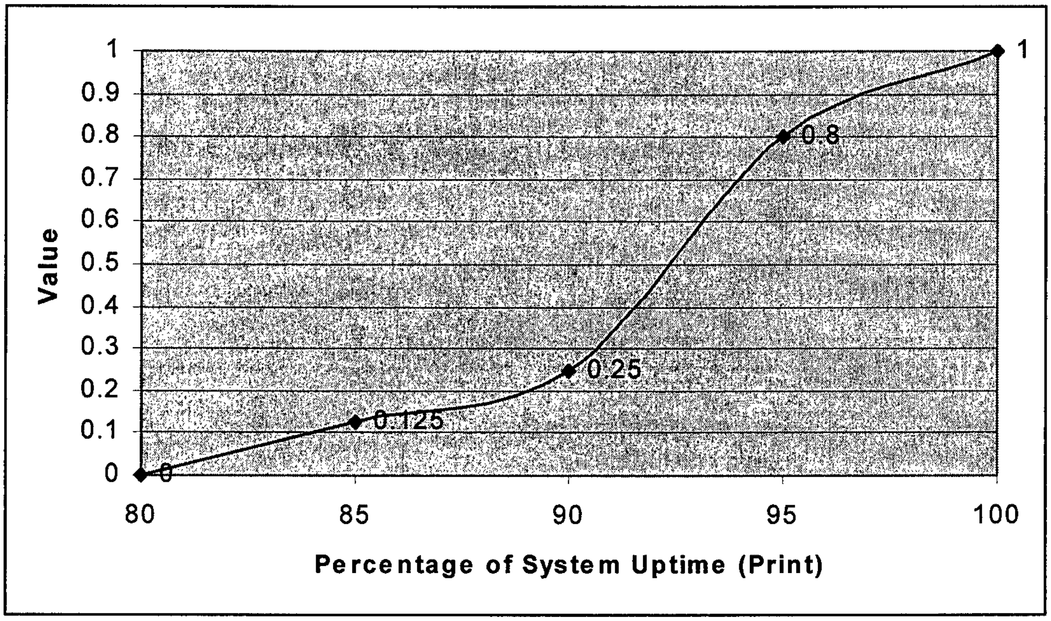


Figure A-6: Percentage of System Uptime (Print)

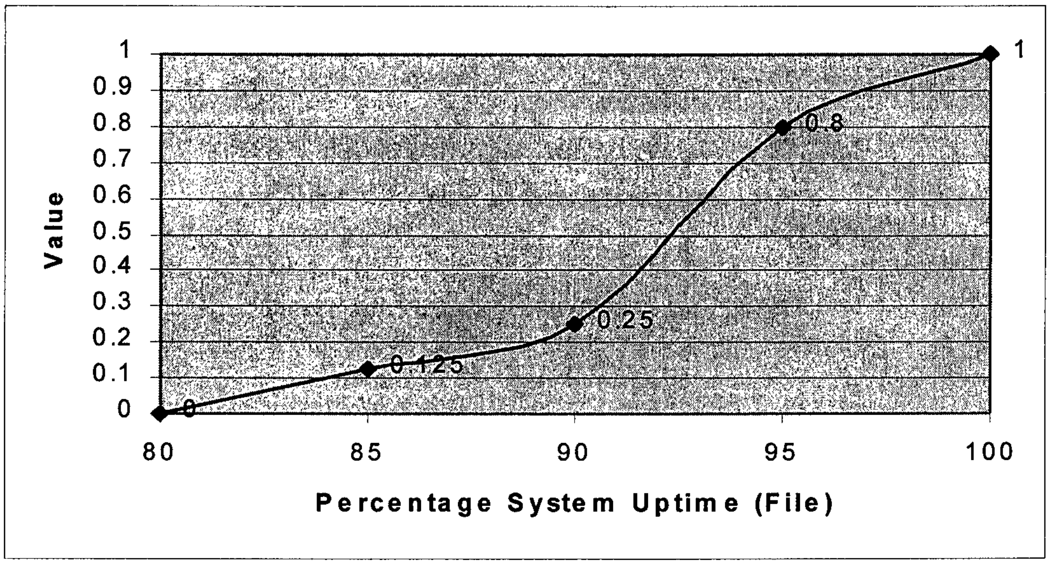


Figure A-7: Percentage of System Uptime (File)

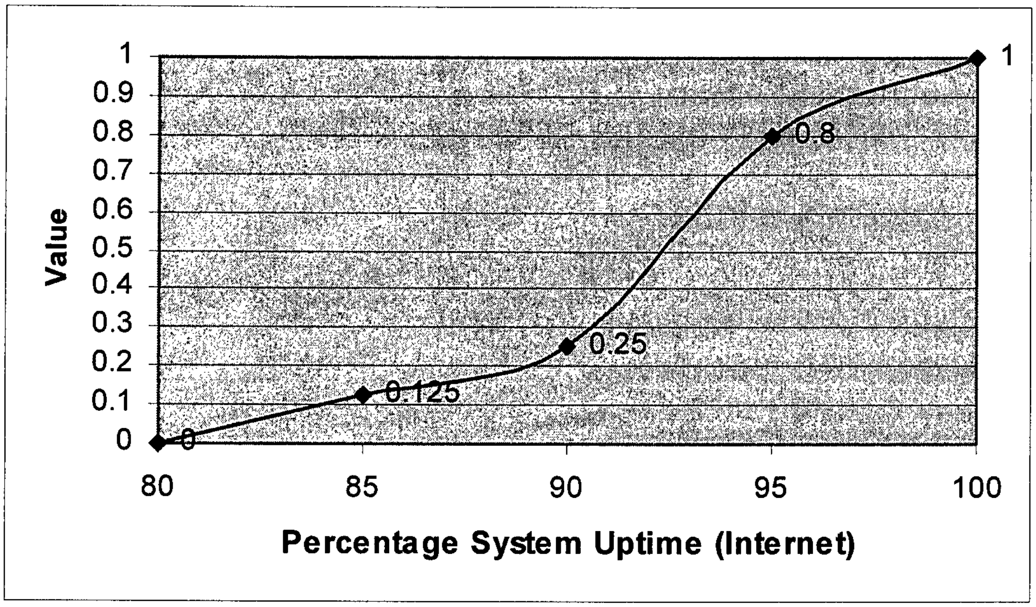
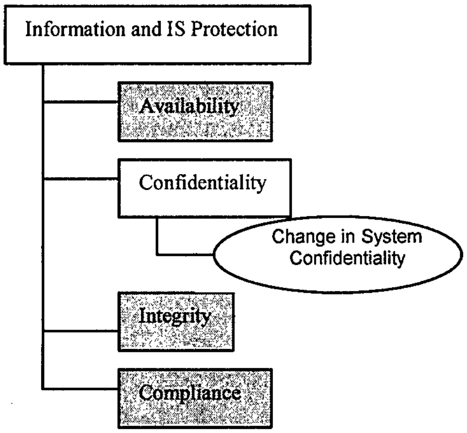


Figure A-8 Percentage of System Uptime (Internet)


Information and IS Protection
Availability
Confidentiality
Change in System Confidentiality
Integrity
Compliance

Confidentiality: Unauthorized people do not have access to restricted information.

Rationale: While Availability considers if system functions are operational, Confidentiality captures whether or not the user is authorized to access the information. It is important that unauthorized people do not gain access to information they should not have. A system that was available 99% of the time to anyone with Internet access would score high in Availability, but it would have no confidentiality. Confidentiality considers both insider access and outsider access. For example, a user with a secret classification should not be able to access a top-secret information system; Confidentiality, as measured here, is therefore independent of who is trying to gain unauthorized access to restricted information.

Measure: Confidentiality is measured by determining what change an IA strategy will have on existing confidentiality. This is done for two reasons: only known confidentiality breaches can be measured (if a breach in confidentiality occurs and is not detected then there is no way of measuring it), and system Confidentiality is not a vulnerability that an organization would necessarily want to disclose. Additionally, confidentiality is rarely constant across a time period. Usually several events will occur that jeopardize confidentiality within a very short time period, which is then followed by a period where no events occur. This is due, in part, to the fact that a particular system vulnerability can be exploited until it is fixed, allowing several events to occur in a short time period. Once fixed, the system is secure again until a new vulnerability is found and exploited. Figure A-9 shows that an IA strategy resulting in No Change to Confidentiality receives a value of 0.5. The categories are linear on either side of No Change since AFTAC values a gain in confidentiality as much as they dislike a loss in confidentiality of a similar magnitude.

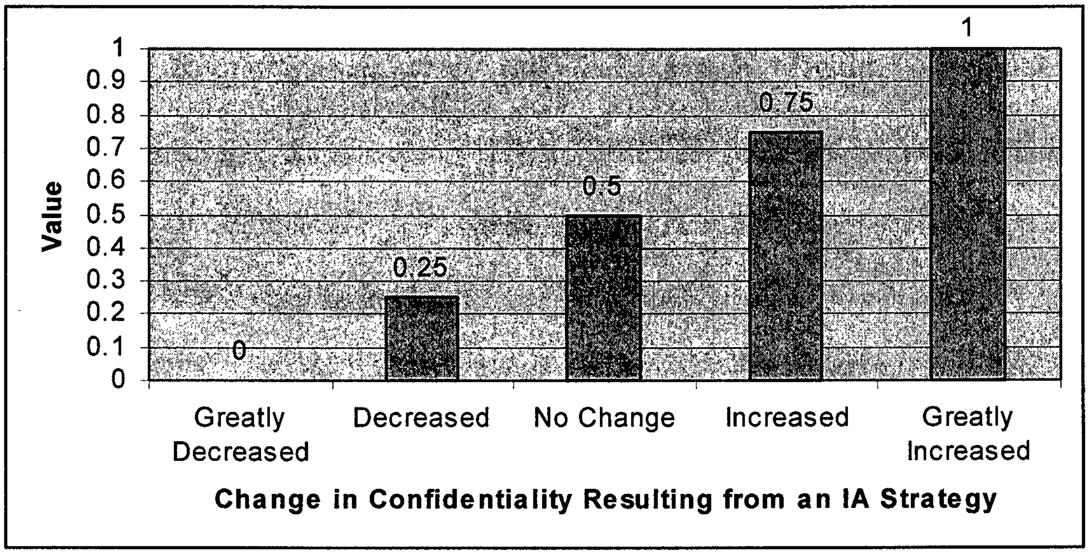
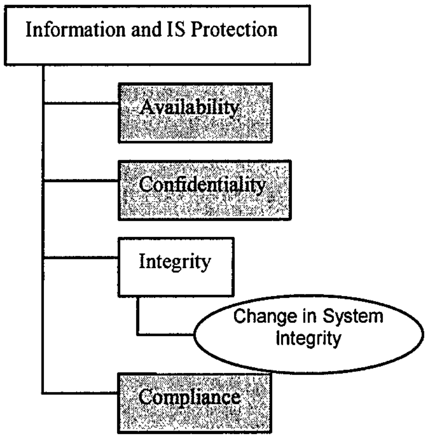


Figure A-9: Change in Confidentiality Resulting from an IA Strategy



Integrity: Protection from unauthorized change.

Rationale: Information in the system must be dependable. It is important that the data in the system be correct in the sense that it is what the originator intended. Integrity addresses the concept that information stored in a database Monday will be the same when accessed on Wednesday. The reasons information could become corrupted are varied; however, whether intentional or unintentional, system integrity must protect against the entire array of possibilities.

Measure: Like Confidentiality, Integrity is also measured as a change from the existing system. Figure A-10 shows that any decrease to current system integrity causes that particular IA strategy to receive a severe value penalty on this measure. Any strategy that either does not affect integrity or increases integrity will score relatively high compared to those that decrease system integrity. The graph therefore shows that a decrease to system integrity has a greater value loss than the gain in value for an increase in system integrity. No Change to system integrity received the score of 0.5.

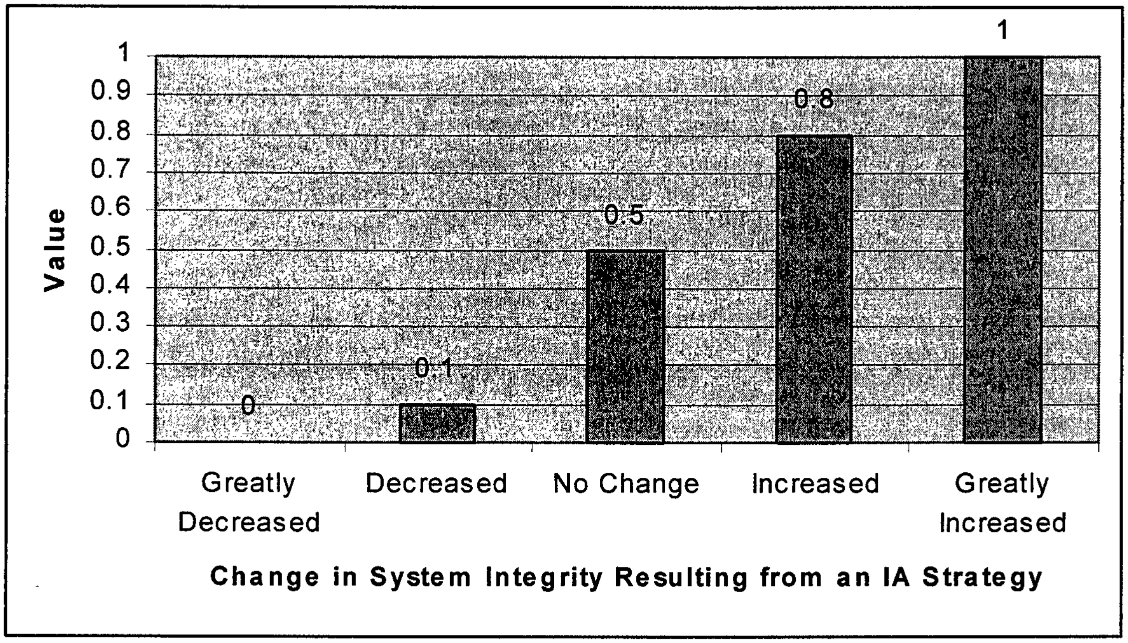
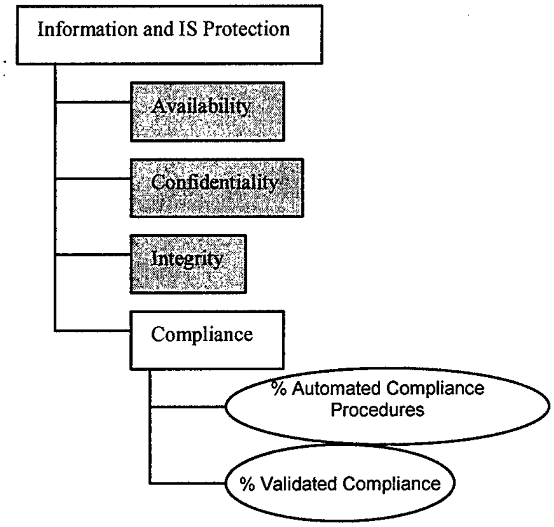


Figure A-10: Change in System Integrity from an IA Strategy

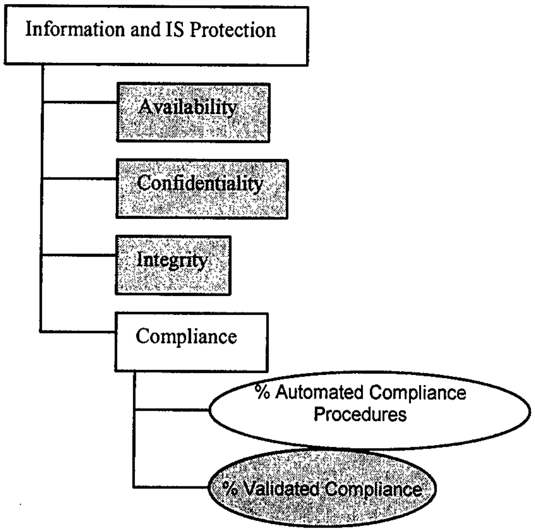


Compliance: Measures taken to protect against known vulnerabilities

Rationale: It is advantageous to an organization to know exactly what security measures have been taken to combat known vulnerabilities. Air Force mandated security programs and policies, such as virus software and AFCERT patches, should be updated regularly to assure the system remains current in its security procedures. It is the duty and responsibility of each agency to comply with Air Force regulations.

Measure: Compliance is measured with two separate functions: the percentage of automated compliance procedures and the percentage of validated compliance.

Percentage of Automated Compliance Procedures:



This measure captures the ability of the system to automatically update and install compliance programs. Automated compliance procedures are advantageous to an organization because they do not require support personnel involvement. This allows procedures to be installed immediately and correctly, in addition to allowing support personnel the ability to concentrate their efforts in other important matters.

The function is linear because it was determined that there is equal value gained for every percentage increase in automated compliance procedures.

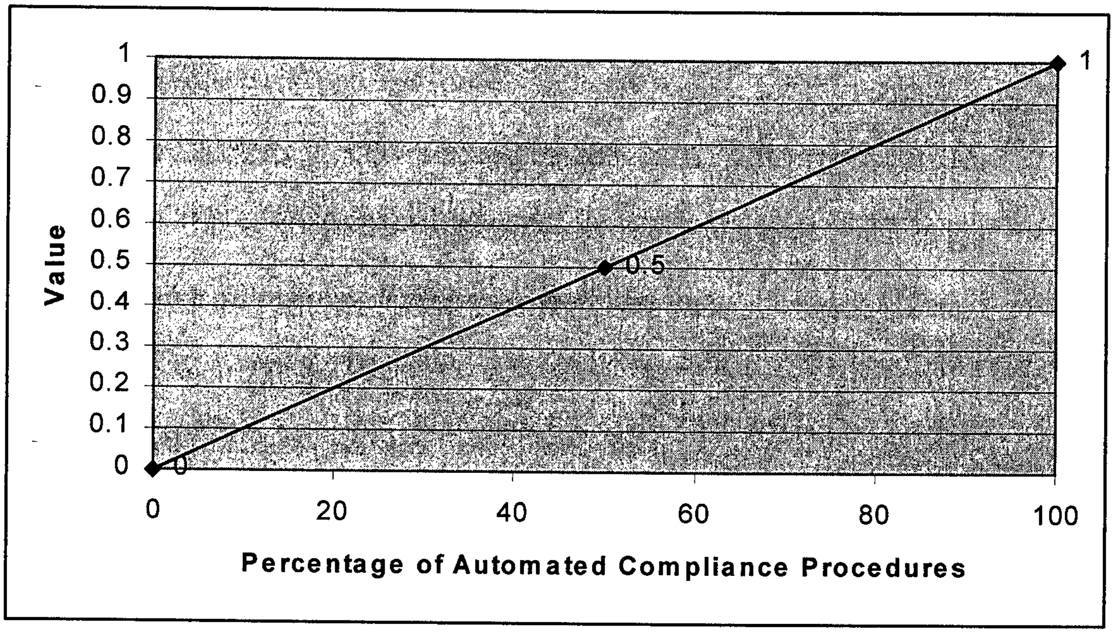
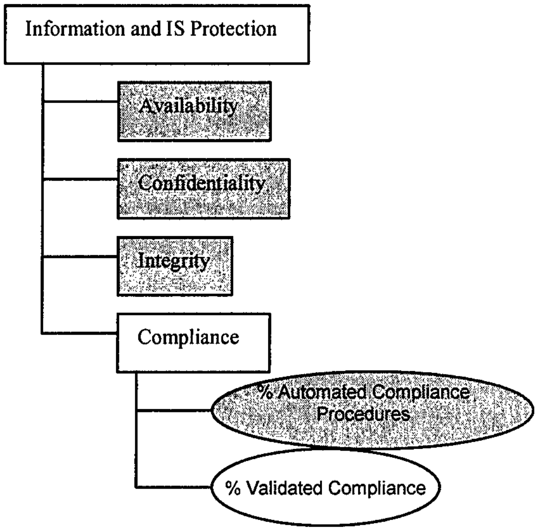


Figure A-11: Percentage of Automated Compliance Procedures



Percentage of Validated Compliance: It is important to know exactly what percentage of compliance procedures an organization has installed. Failure to install these procedures could lead to an unnecessary information compromise. This measure is shaped as an S-curve with a sharp upward trend at 75% because AFTAC experts feel that a system with less than this percentage of validated compliance provides little value to system protection. At 90% the curve flattens, meaning that increasing the percentage of validated compliance above this level results in smaller marginal value gains to system protection.

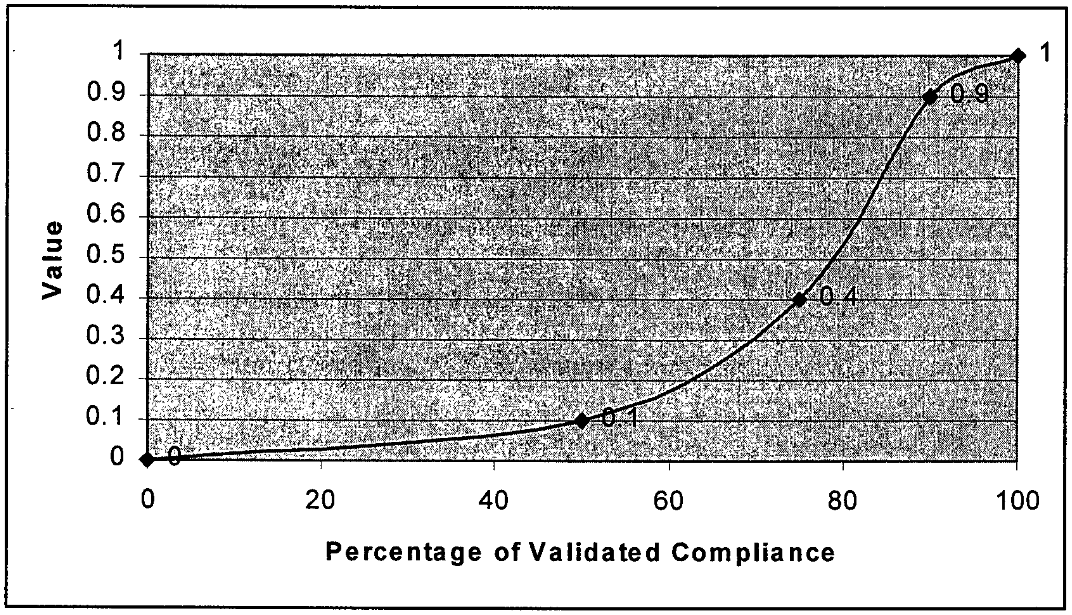


Figure A-12: Percentage of Validated Compliance

The next sub-hierarchy under Information Assurance is Detection. Figure A-13 shows the complete Detection sub-hierarchy.

Detection

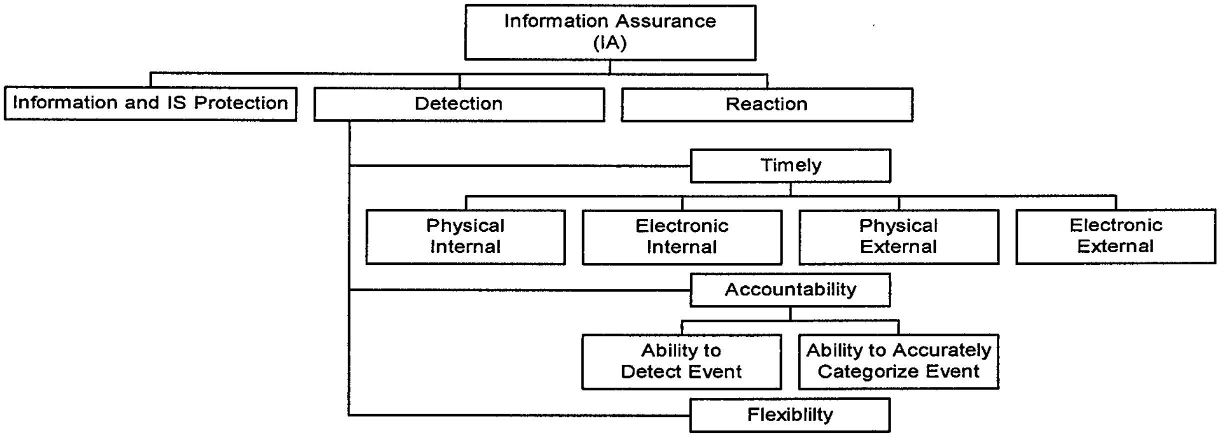


Figure A-13: Detection

Detection: The ability of the system or system personnel to detect an event. Again, an event is any abnormal activity or action that could compromise the system or information contained within the system.

Rationale: The system's ability to quickly and accurately detect an event is valued because an event cannot be stopped unless it is first detected. Detection is further decomposed into Timely, Accountability, and Flexibility. Detection can occur from either system personnel or the system itself. Detection capabilities must also have the ability to be increased or decreased depending on the INFOCON situation (reference Chapter 2). To measure this ability, Flexibility is included under Detection.

Timely

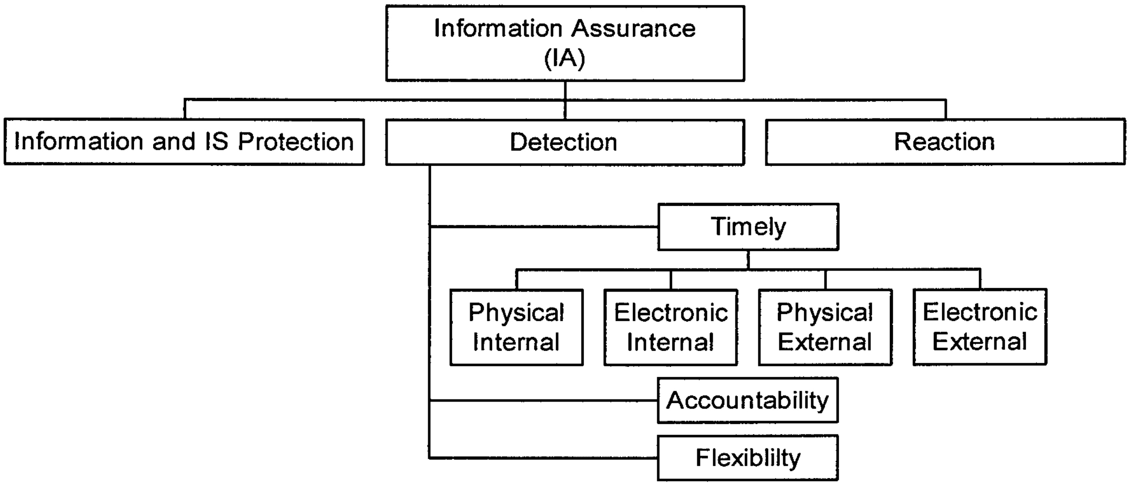
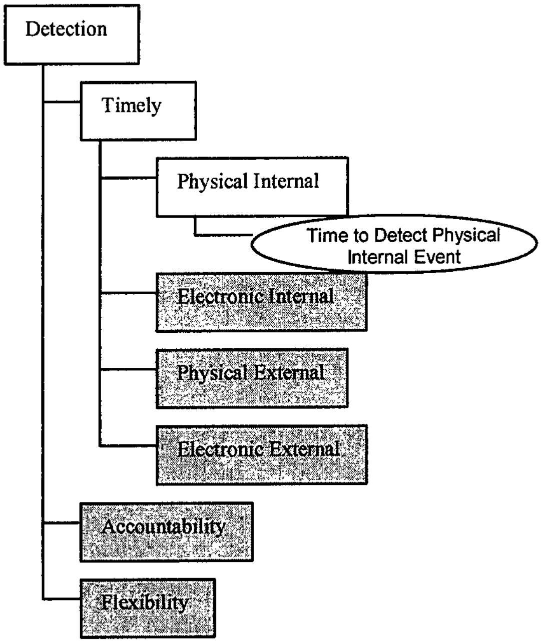


Figure A-14: Timely

Timely: The amount of time it takes to detect an event. The amount of time is measured from the actual start of the event (which may or may not be immediately known) to the point of detection.

Rationale: If an event can continue undetected for an extended period of time (extended being relative to the system and the type of event), then that event has a greater opportunity to cause harm than an event that was detected immediately. Since different events may take a different amount of time to detect or pose a different type of threat, Timely was separated into Physical Internal, Electronic Internal, Physical External, and Electronic External. An internal event is any event caused by a person authorized to use or work around sensitive information. An intrusion by a janitor who steals information while cleaning after hours would therefore be classified as an internal event since he was authorized to be around valuable information, although he would not have been approved to access it. An authorized user is a person who is trusted to view, edit, or otherwise manipulate the information; having access to a facility, like the janitor in the above example, does not necessarily mean that person is authorized to use a system in the facility. An external event is any event caused by personnel outside of the AFATC organization that harms the system or system information. Again, an event does not have to be malicious; a construction crew that is working outside the AFTAC building and accidentally cuts an AFTAC phone line would be classified as an external event. Physical events are situations where physical property is damaged, while electronic events are strictly performed through computer networks.



Physical Internal: A physical disruption of the information or IS by a person within the organization. This could be either accidental (spilling coffee on a keyboard causing the system to short) or intentional (breaking the lobby keypad to obtain access to a restricted area).

Rationale: Measures must be taken to prevent internal physical events, whether intentional or accidental, that could result in a compromise of information. Whether the event was malicious or not is irrelevant for this measure; it must be detected in a timely fashion so that proper action may be taken.

Measure: The time to detect physical internal events is measured in eight-hour working days since, in the vast majority of instances for AMIS, the event is not malicious and valuable information is not lost or stolen. There is a steep drop after five working days since AFTAC personnel view one workweek as sufficient time to detect a physical internal event. There is still some value in detecting the event prior to ten working days, but the curve flattens out rapidly. At twenty workdays (one work month), AFTAC personnel feel that more than sufficient time had passed since the event actually occurred, and detecting it beyond this point, while necessary, does not score any value.

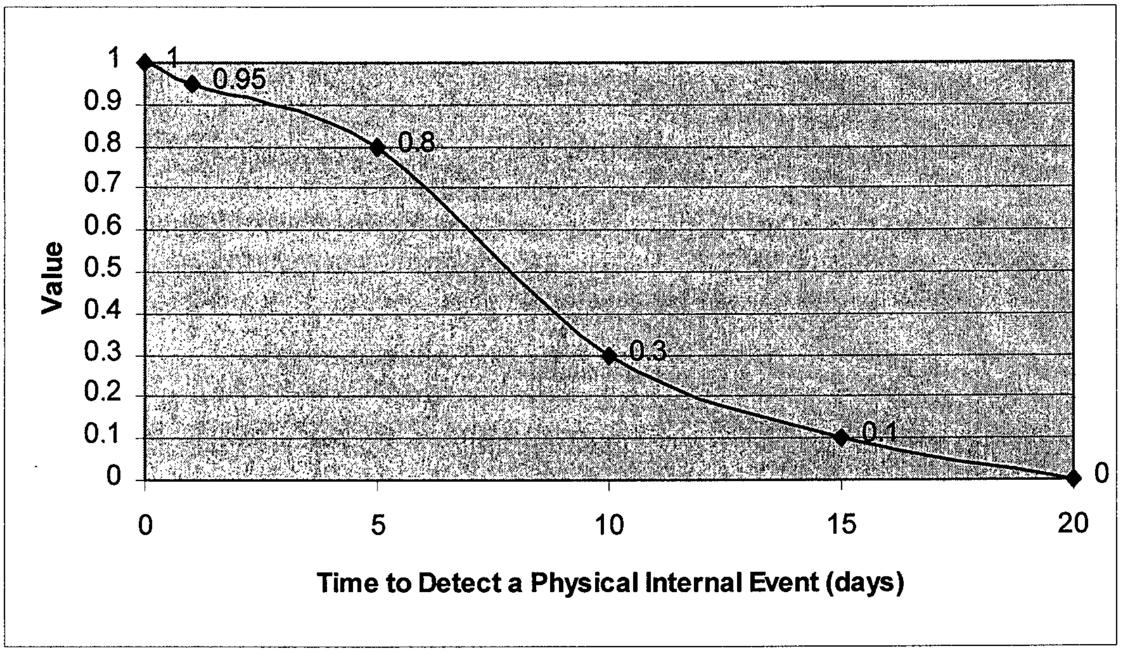
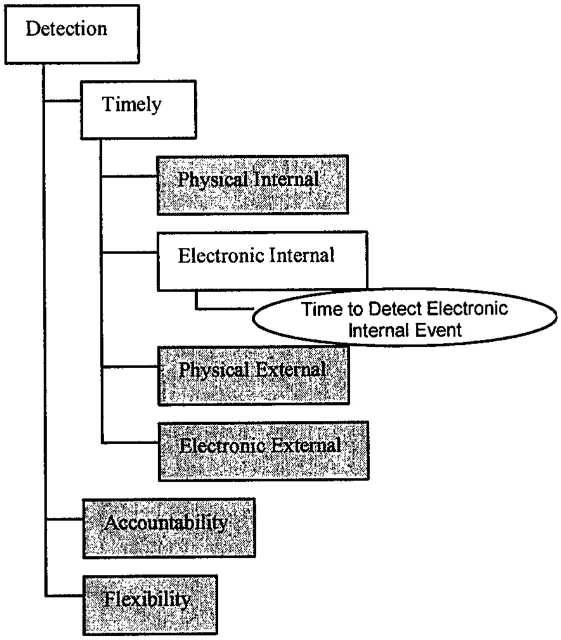


Figure A-15: Time to Detect a Physical Internal Event, measured in eight-hour workdays

Electronic Internal: An electronic event originated from an internal source, whether intentional (purposely trying to login to a system above the user's classification) or unintentional (accidentally accessing a restricted site) that could compromise information.



Rationale: A tremendous amount of information can be compromised, lost, or stolen depending on the type of electronic event that may occur. It is therefore necessary to detect these types of events as quickly as possible.

Measure: Since Electronic Internal events originate from a "friendly source," who are assumed to be responsible and dedicated employees, this value is measured in eight-hour workdays. Air Force personnel are trusted to make the right decisions regarding sensitive information, and therefore they are not continuously monitored. However, since the opportunity exists to lose sensitive information quickly, electronic internal events must be detected more rapidly than physical internal events. There is a fairly steep curve from immediate detection to one day since there is great value in the ability to detect this type of event as close to the time that it occurred as possible. The curve flattens after one day but up until a week (5 days is one workweek) because there is still high value in detecting an event rapidly. After one week, the curve is essentially linear meaning that each day is as important as the next, scoring nothing at 10 or more workdays.

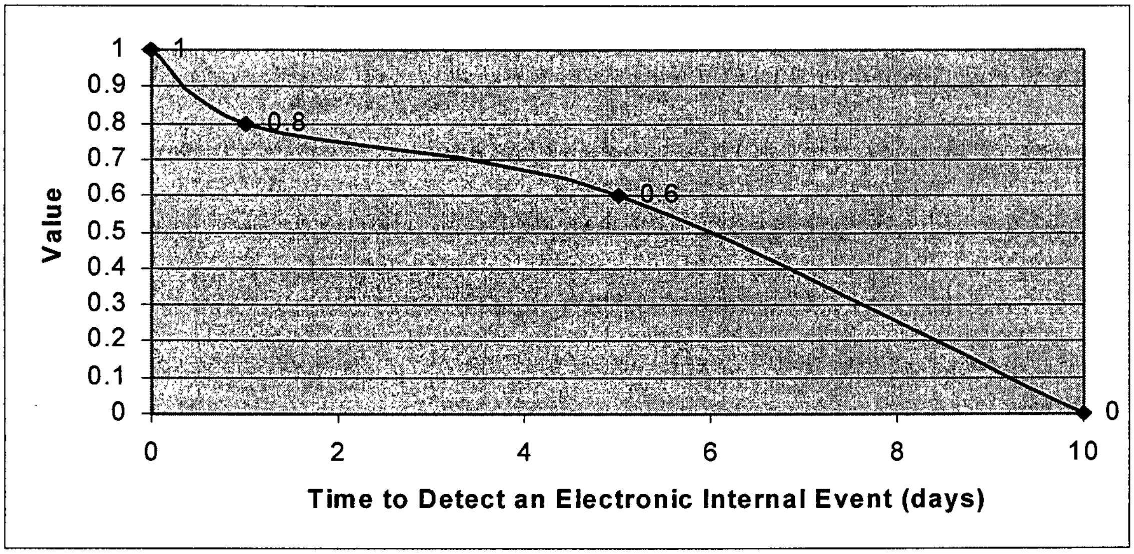
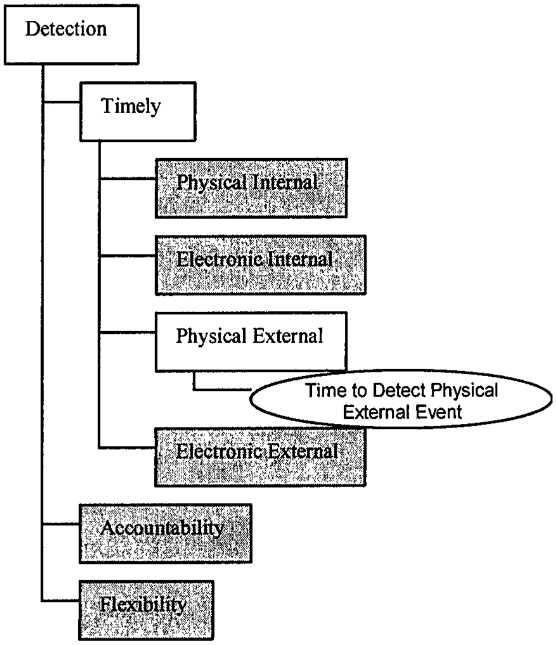


Figure A-16: Time to Detect an Electronic Internal Event, measured in eight-hour workdays

Physical External: Any physical event affecting the information or IS by an outside individual.



Rationale: An external physical event is defined as any event originating from persons outside the AFTAC organization that harms AFTAC property. It is irrelevant, in terms of the measure of detection, if the event was malicious in nature or not. A construction crew who accidentally cut the phone line outside the building or a group posing as a construction crew who maliciously destroyed the line both cause the same initial damage and therefore requires the same timely detection.

Measure: The time to detect a physical external event is measured in hours due to the fact that any event originating from an outside source is deemed to be of much higher potential threat than an event originating within AFTAC. A physical event could cause any number of problems for AFTAC, ranging from loss of communication to damaged computers, or even damage to personnel in the most extreme cases. It is therefore necessary to detect these types of events as close to their actual occurrence as possible. The graph illustrates this point by showing that approximately half the value is lost after only one hour, three quarters of the value is lost at two hours, and no value at all is earned if the system or system personnel cannot detect the event within one work day (eight hours).

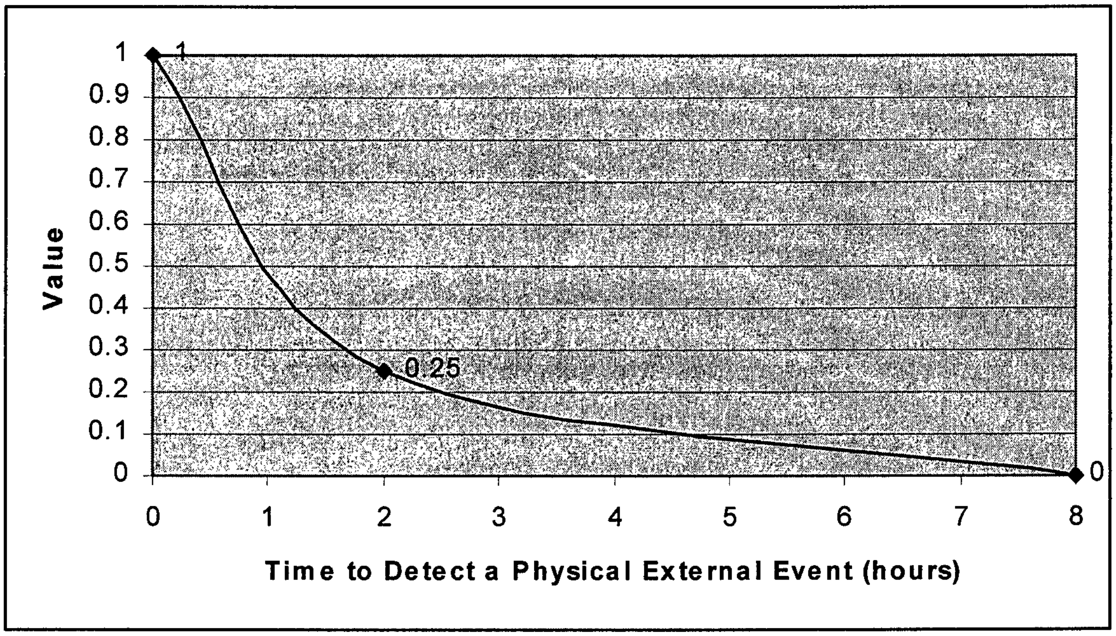
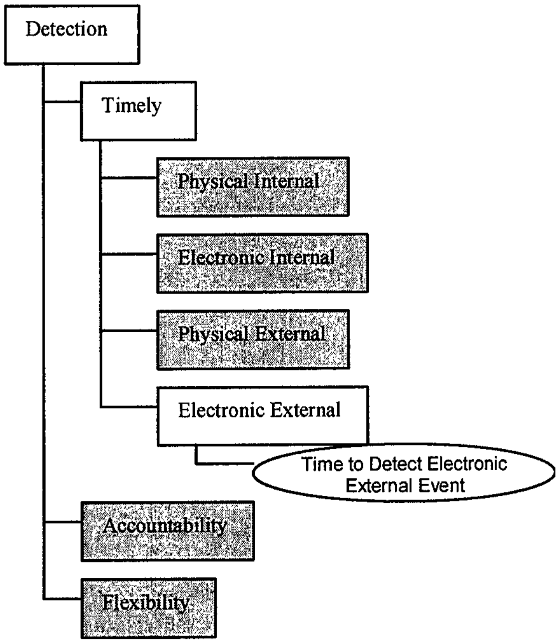


Figure A-17: Time to Detect Physical External Event, measured in hours



<u>Electronic External:</u> An electronic event originating from an external source that could compromise information, harm the system, or be otherwise disruptive to the mission.

<u>Rationale:</u> Any attempt to gain access, destroy, or otherwise compromise the system from an outside source must be detected as quickly as possible to eliminate the possibility of an attacker gaining valuable information or, worse, going unnoticed. Electronic external events are the most dangerous events from an information assurance point of view because they are hard to detect, they are often malicious attempts to damage or steal AFTAC information, and they can happen very rapidly.

Measure: Electronic external events are measured in minutes because of the extreme threat they pose to a system. Like physical external events, there is a tremendous loss in value if the event cannot be detected immediately; after only 10 minutes the system will receive a score of 0.5 and by the one-hour point less than a score of 0.1 is assigned. If the system cannot detect an electronic external event within two hours, then it is seen as totally unacceptable and gains no value.

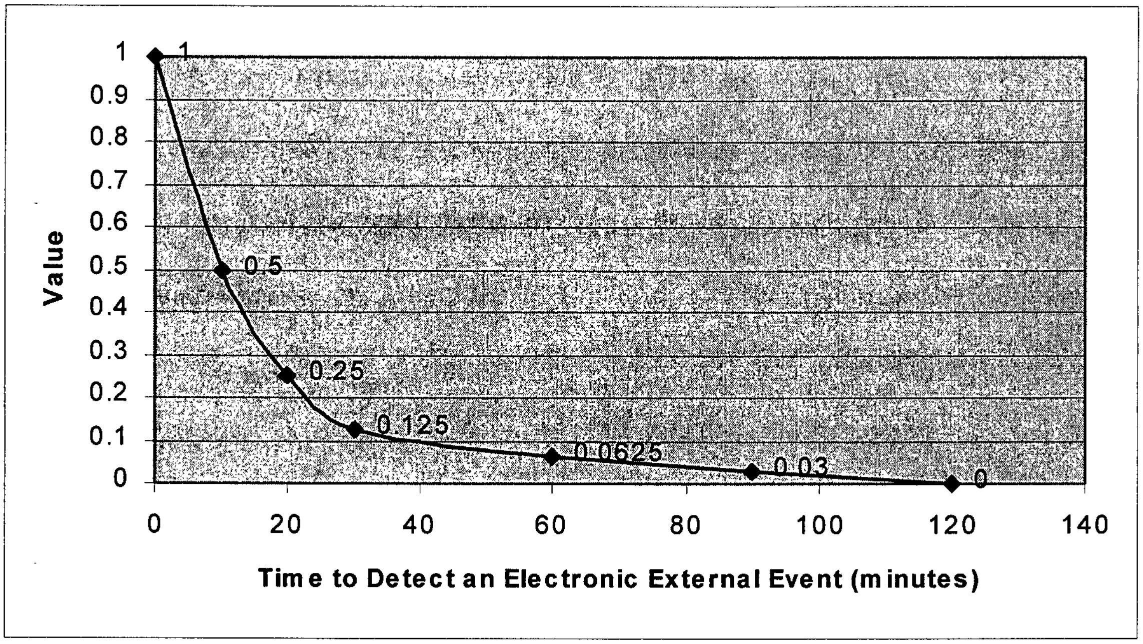


Figure A-18: Time to Detect a Electronic Internal Event, measured in minutes

Accountability

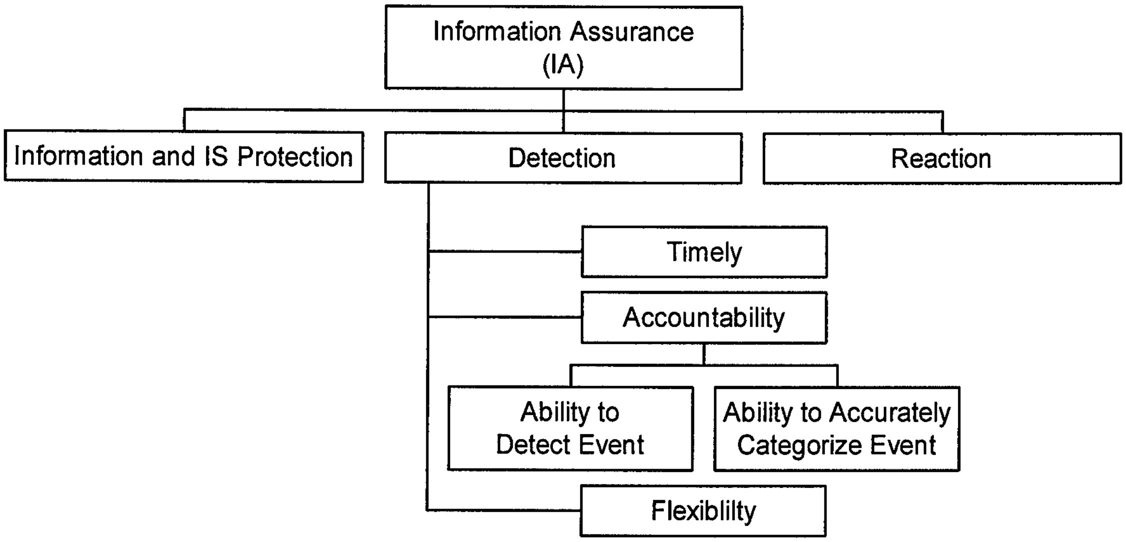

Information Assurance (IA)
Information and IS Protection
Detection
Reaction
Timely
Accountability
Ability to Detect Event
Ability to Accurately Categorize Event
Flexiblilty

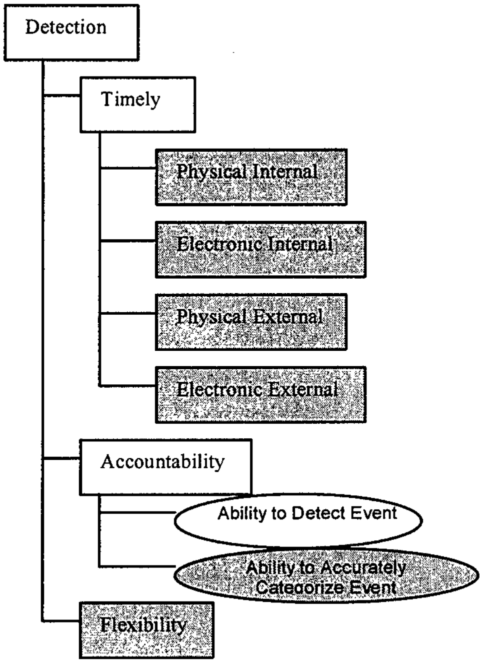
Figure A-19: Accountability

Accountability: The ability of the system to detect and correctly classify events.

Rationale: Accountability is composed of two sublevels that are classified separately because they carry different levels of importance. An event must first be detected as an event and then categorized properly. Failure to do either of these could result in an event (1) going unnoticed, or (2) thinking an event was one type of activity when in reality it was another and thus resulting in an improper reaction. A system cannot be fully accountable if it does not perform both of these values proficiently.

Ability to Detect an Event: The ability of the system or system personnel to determine if an event occurred.

Rationale: An event must first be detected in order to determine if it was malicious, what information was



compromised, and who was responsible. If the event is not detected then valuable information may be compromised for an indefinite period of time.

Measure: Since the detection rate (percentage of events detected) is impossible to calculate (the system and system personnel may never know of events they did not detect), the assumption is made that a fully automated detection system will be more effective than a fully manual detection system. For example, a system that has the ability to automatically detect unauthorized user intrusions is more valuable than one that requires support personnel to periodically check log files for abnormalities. The graph shows that a system with 100% automated detection capabilities receives a score of 1.0, and a system relying completely on human detection (0% automated detection capabilities) will receive a 0.0. It is assumed that a system with 25% automated detection capabilities has 75% manual detection capabilities. The fractions represent the percentage of total time spent on detecting events; therefore 50% automated and 50% manual would mean that machines and personnel would spend the same amount of time detecting events. The line between the two endpoints is slightly convex showing that AFTAC prefers more automated systems to more manual systems.

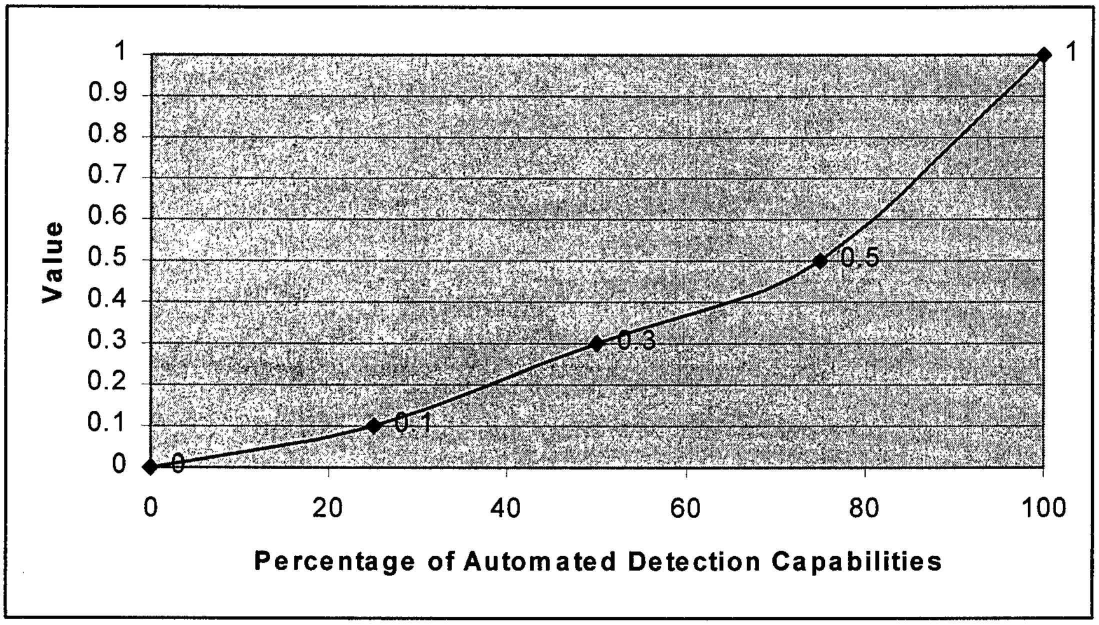
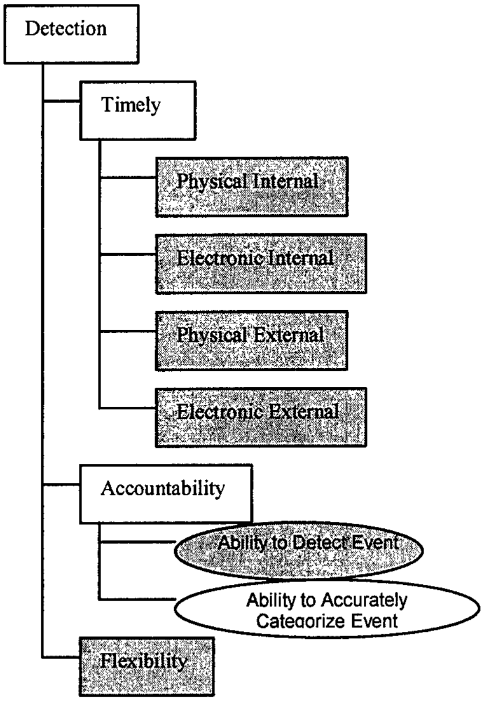


Figure A-20: Ability to Detect an Event, measured by Percentage of Automated Detection Capabilities

<u>Ability to Accurately Categorize an Event:</u> The ability of the system or system personnel to categorize an event correctly.



<u>Rationale:</u> If the event was not categorized correctly, then reaction to the event may be improper. An over reaction (i.e. "pulling the plug") may impact mission capability and therefore is extremely undesirable, while an under reaction (or perhaps no reaction) may result in permanently lost or damaged information, an even worse outcome.

<u>Measure:</u> The identical categories were used for this measure as were used in the Ability to Detect an Event measure for the same rationale. Automated systems can categorize more events in a shorter period of time than humans. For example, a machine can read through system logs much faster than a person can, so it would be expected that a machine could categorize more errors in the logs than a human could. The shape of the curve is similar to that of the Ability to Detect an Event, showing that the jump from 75% automated to greater than 75% automation is valued more than any other jump of the same distance.

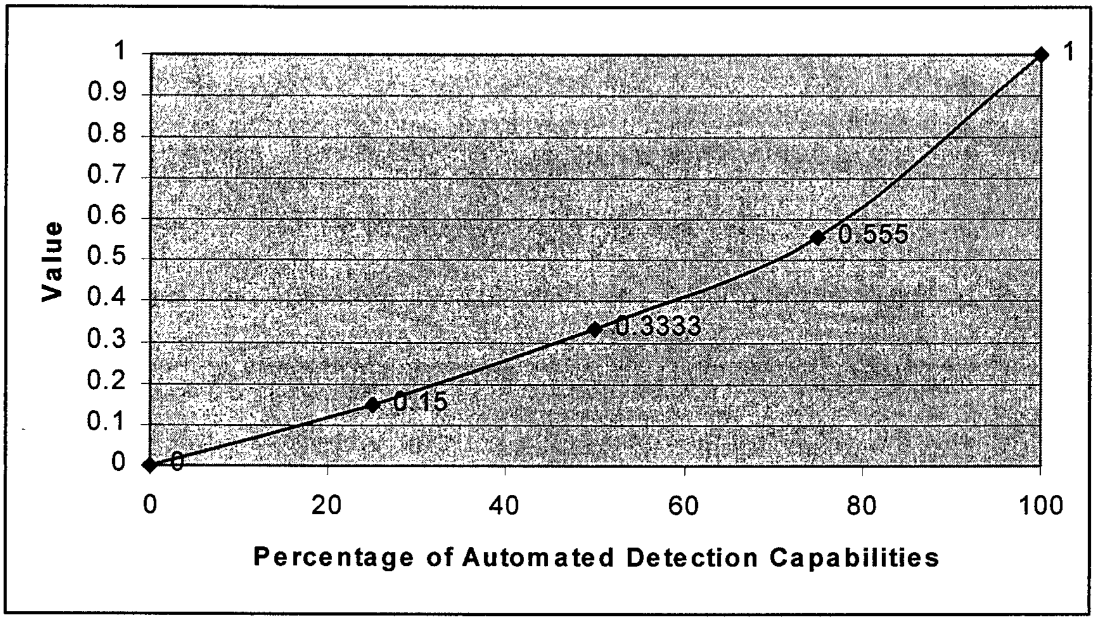
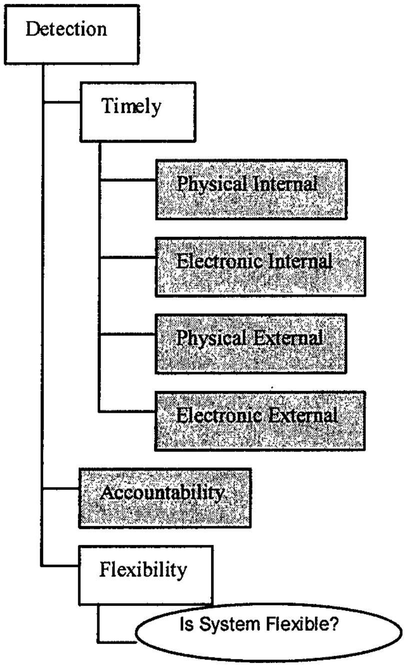


Figure A-21: Ability to Categorize an Event, measured by the means of detection



Flexibility: The ability of the system to increase or decrease detection capabilities depending on the situation at hand.

Rationale: It would be advantageous for a system to have the capability to increase or decrease its detection capabilities based on the current INFOCON level. For example, at INFOCON ALPHA, the detection capabilities of the system might operate at normal. If the organization should then go to INFOCON BRAVO, it would be beneficial to have the ability to adjust detection capabilities in order to reach higher detection fidelity. This would allow the system and system personnel to detect more events in a high threat environment than it would in a low threat environment.

Measure: This measure is a simple yes / no because the system either has the capability to increase or decrease detection capabilities or it does not. An inflexible system would be a system that could only be on or off, whereas a flexible system would have the ability to turn certain functions on or off, or change the level of detection at which certain services function. For example, a system that could shut down e-mail while keeping the print server active would be a flexible system. A system which could be set to stop more suspicious traffic according to INFOCON levels would be valued. At a low threat level, the number of false positives could be kept low. In a higher threat setting, requiring greater vigilance, the system would regularly have a higher false positive level, which is acceptable in high threat situation but not acceptable for normal operations.

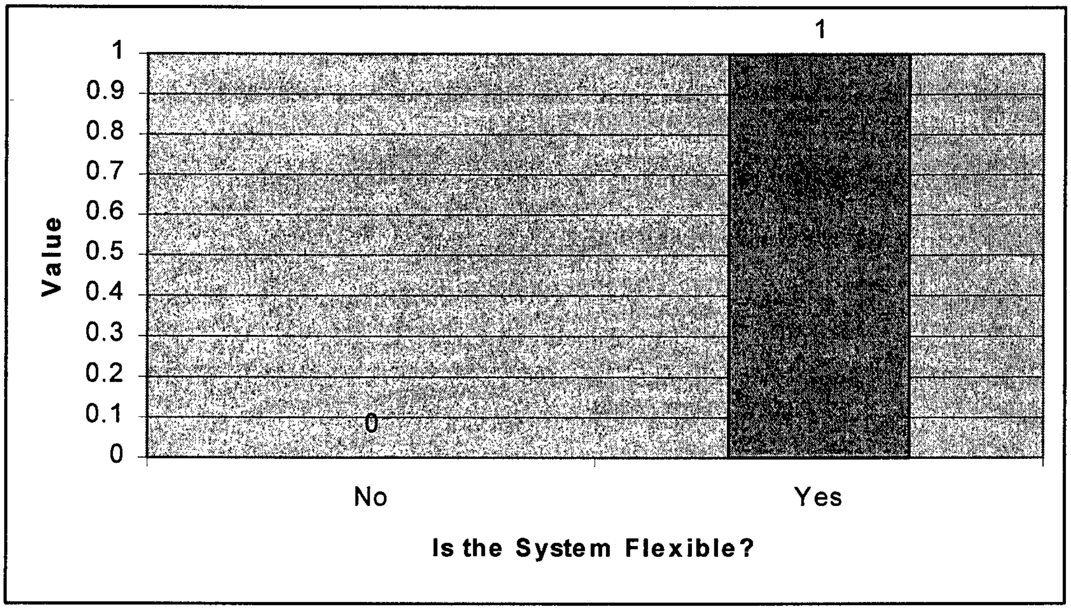


Figure A-22: System Flexibility

Reaction

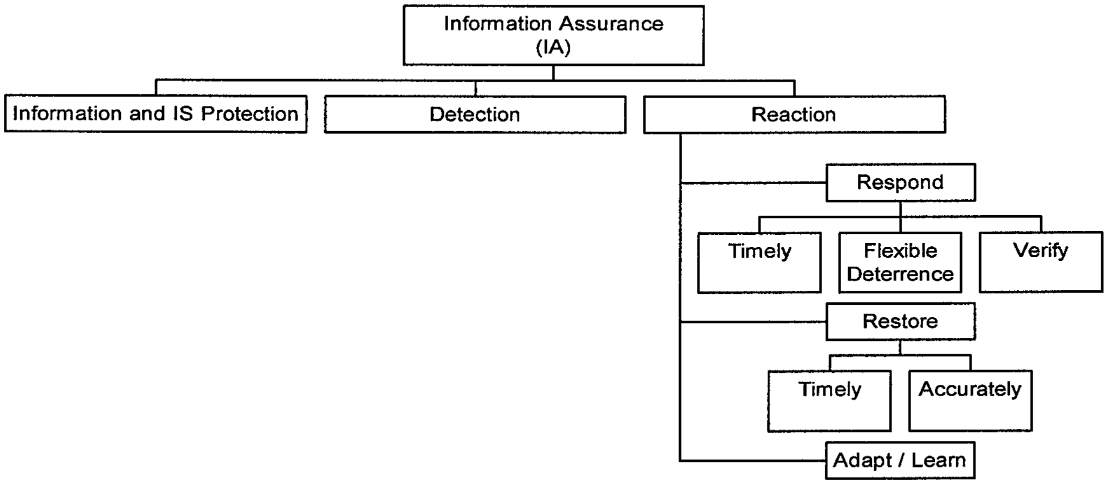


Figure A-23: Reaction

Reaction: Measures taken to (1) appropriately respond to an identified attack and (2) restore the information and IS capabilities to an acceptable state, their original state, or an improved state. Reaction also includes the ability to learn from previous events so that the likelihood of future damage is reduced or eliminated for that type of event.

Rationale: The third step in assuring information is to properly react to an event. If there is no action taken once an event has occurred, then the event could continue indefinitely. Reaction involves three separate values: the ability to Respond to the event, Restore the information, and Adapt to the new situation. Again, the Reaction sub-hierarchy is not meant to be a timeline; Respond, Restore, and React are values that were developed based on joint doctrine and the opinion of AFTAC personnel because they are considered important elements of information assurance.

Respond

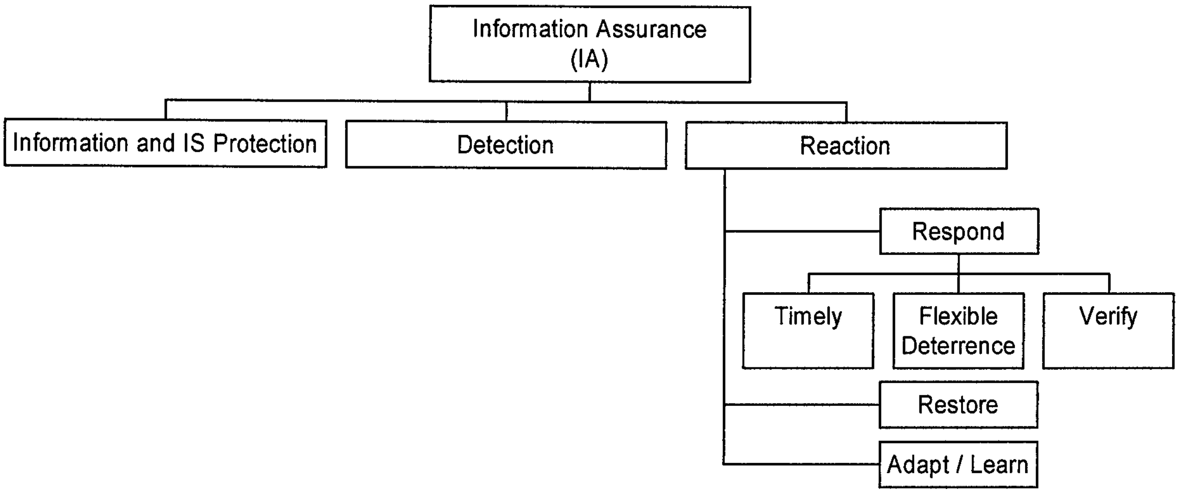
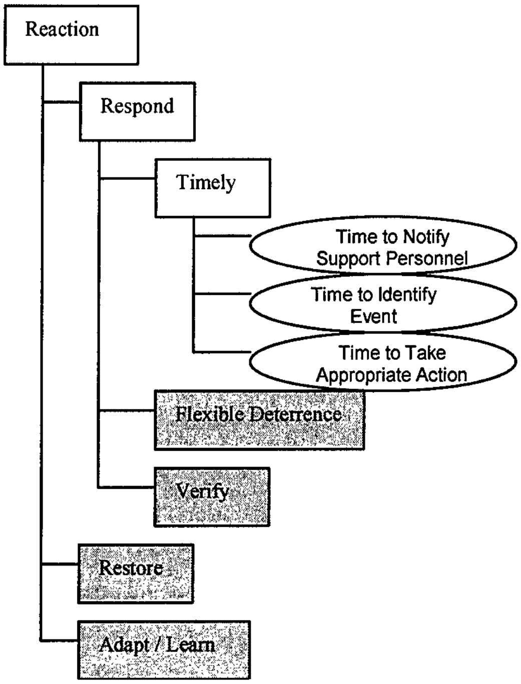


Figure A-24: Respond

Respond: The ability to take proper action after an event is detected

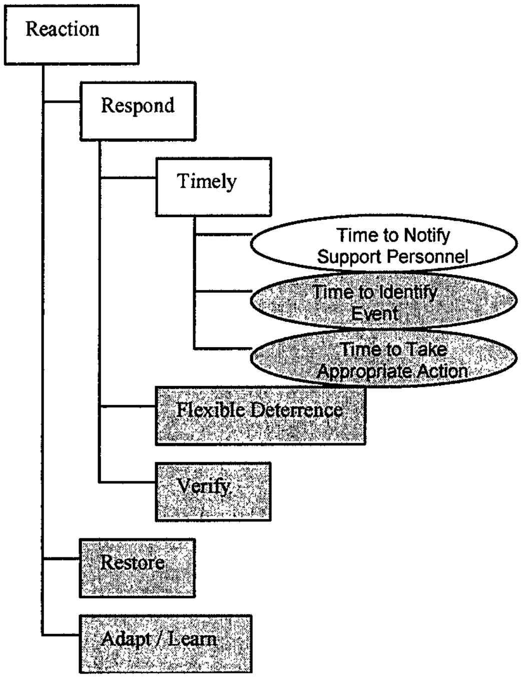
Rationale: Once an event is detected, failure to take proper action could allow the event to continue, cause other events to occur, or possibly ruin a chance to prosecute an attacker. It should be noted that AFTAC is not authorized to launch any offensive actions; however they must report the incident to a higher authority who may then take appropriate action, as they deem necessary. AFTAC does have a responsibility to take defensive actions to assure its information and information systems. In addition, they also have a responsibility to collect appropriate information during an event to aid AFTAC and others in taking authorized steps in response to the event. Respond is therefore broken down into Timely, Flexible Deterrence, and Verify.

Timely: The time needed to notify appropriate personnel after detecting an event, identifying the event source, and then taking the proper action against the event.



Rationale: It is essential to know exactly who is responsible for an event and what damage the event caused. Notifying system personnel and identifying the parties involved in a timely fashion makes personnel aware that a certain group or individual may be trying to access unauthorized information.

Measure: The time it takes to correctly respond to an event. This measure is broken into three separate parts: Time to Notify Support Personnel, Time to Identify the Event, and the Time Needed to Take Appropriate Action.



Time to Notify Support Personnel: The time it takes from the discovery of an event until support personnel can be notified. The most desired occurrence is that the proper support personnel are instantaneously and directly notified; for instance proper personnel are immediately paged as soon as the system detects an event. The next best category is that they are instantaneously but indirectly notified, an example being that support personnel receive an e-mail alert at the same time the system detects an event. The final three categories are notification by support personnel (they discover the event and are therefore notified upon discovery), a user detecting the event (not valued as much since the user must then notify the support personnel), and finally the worst being no notification whatsoever.

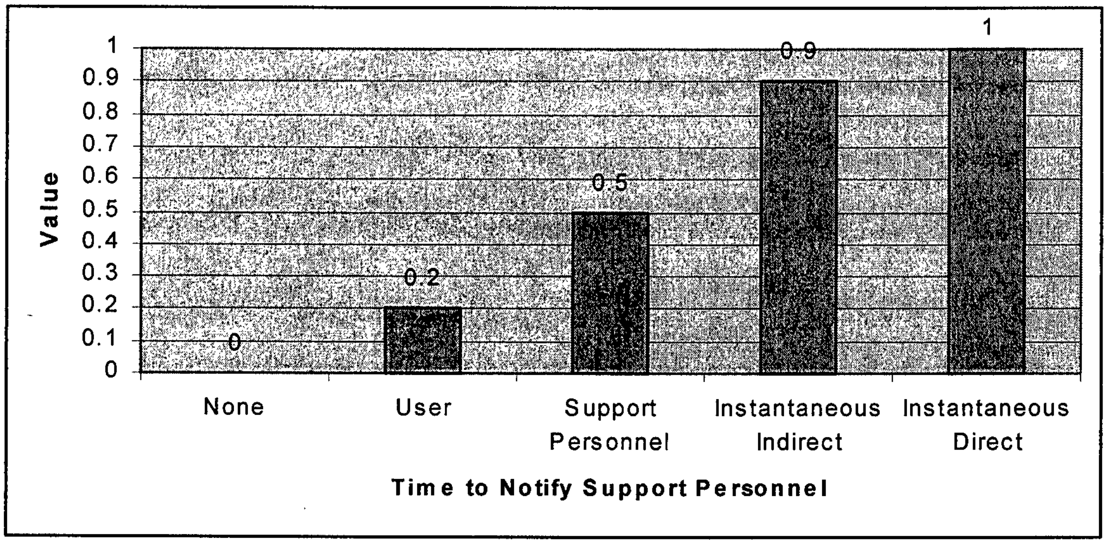
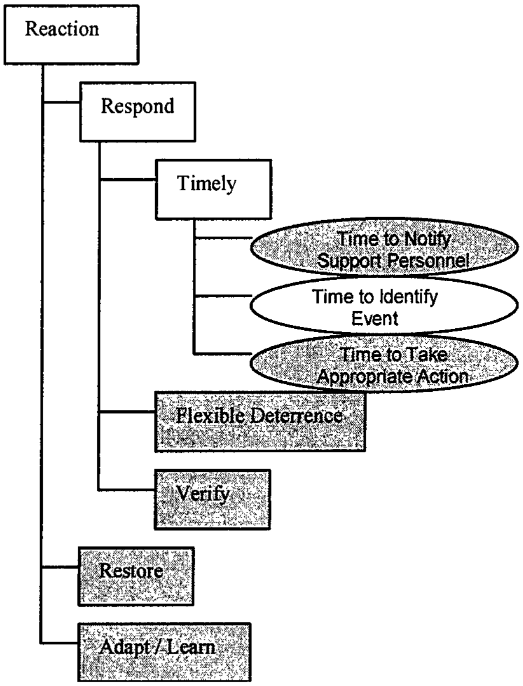


Figure A-25: Time to Notify Support Personnel

<u>Time to Correctly Identify an Event:</u> Measured from the time support personnel have been notified until the time they correctly determine the nature of the event. Any correct identification after two hours, while necessary, is deemed too slow to be valued.



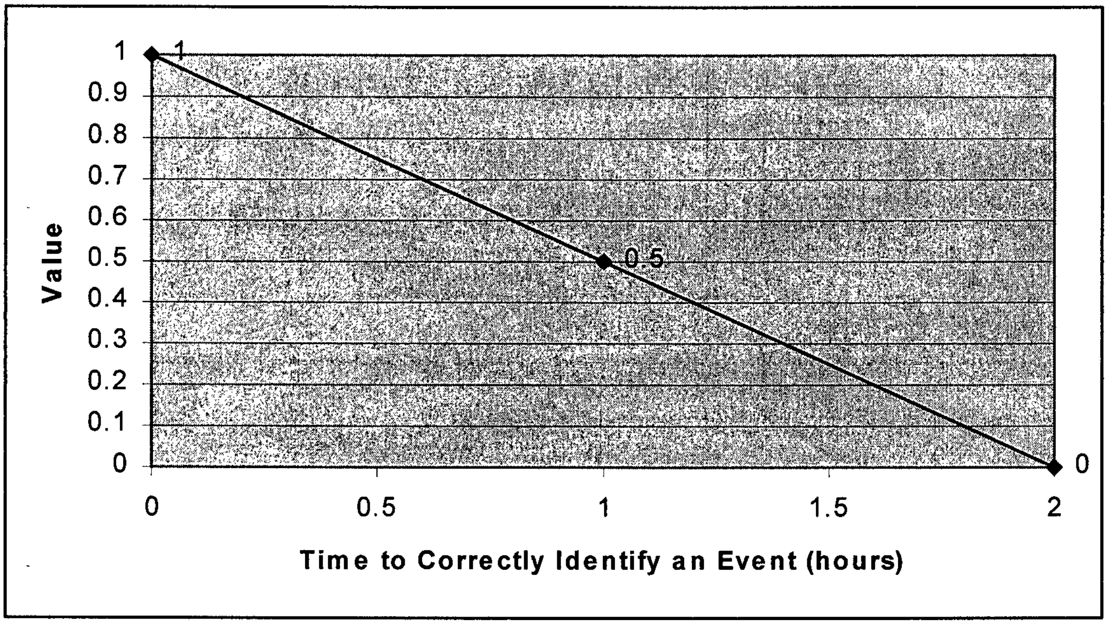
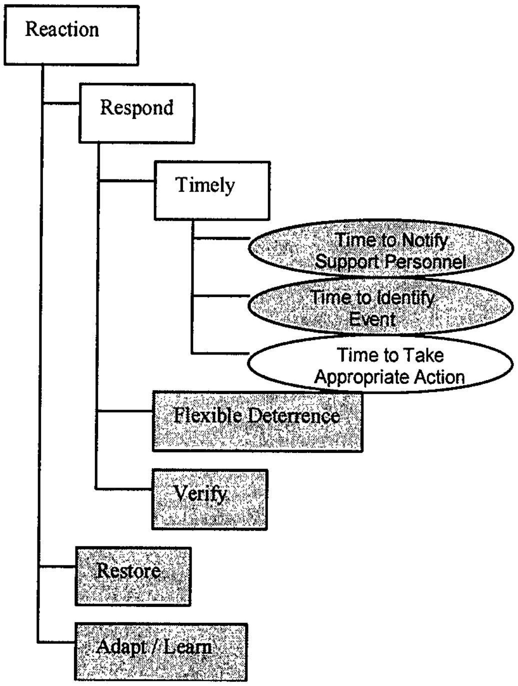


Figure A-26: Time to Correctly Identify an Event, measured in hours

Time to Take Appropriate Action: Measured from the time the event was correctly identified until the situation is under control of system personnel (control implies either stopping the event, containing the event, or *intentionally* prolonging the event to gather evidence). If the time to take proper action is sixty minutes or more, a score of zero will be given

.



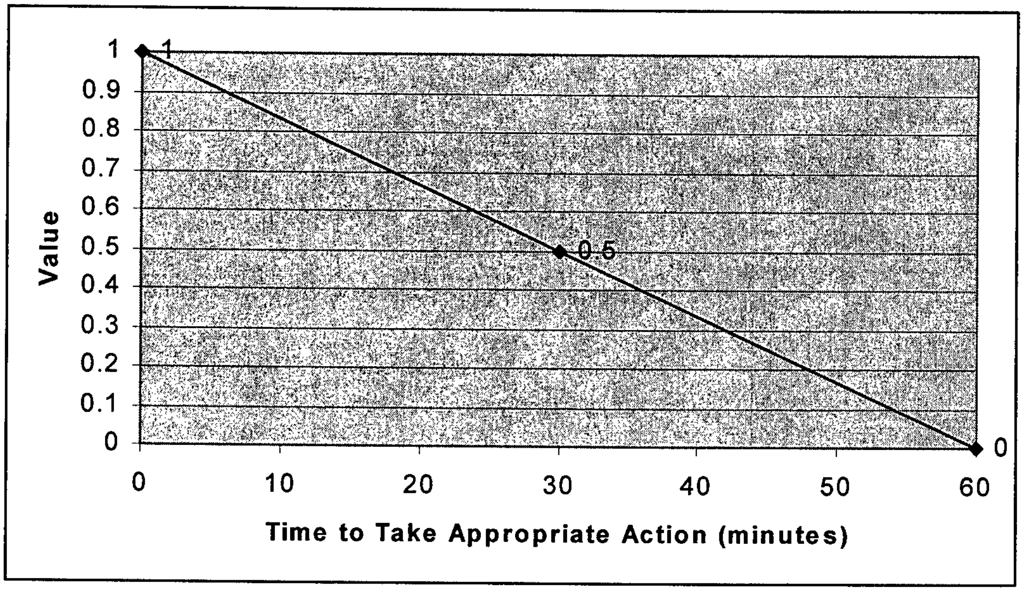
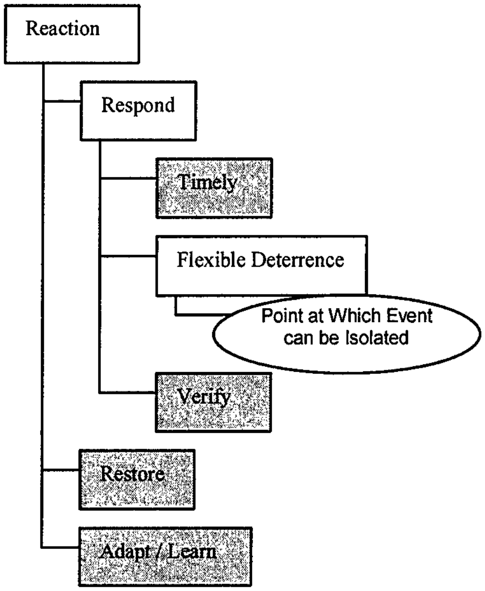


Figure A-27: Time to Take Proper Action, measured in minutes



Flexible Deterrence: Taking appropriate action at the appropriate time.

Rationale: Almost any event can be stopped by completely shutting down the system. However, this may not always be the best course of action since (1) essential missions will be impacted, and (2) it may prevent the collection of evidence necessary for future prosecution. The ability to have graceful degradation, where the system can be taken down in steps rather than all at once, is therefore necessary to take proper action.

Measure: This measure is separated into categories that classify the system's ability to be shut down at different levels. The preferred outcome is a system that will disconnect from the network only at the source of an event, causing minimal disruption to the rest of the system and its users. The worst case is that during any event, the entire system must be shut down. High value is still gained if the event can be isolated at the service level, for instance the system administrators can shut down the print service if an event is detected within that server. Very low value is given if the entire server must be taken down in order to isolate an event since it will now be unavailable to all who need to use it.

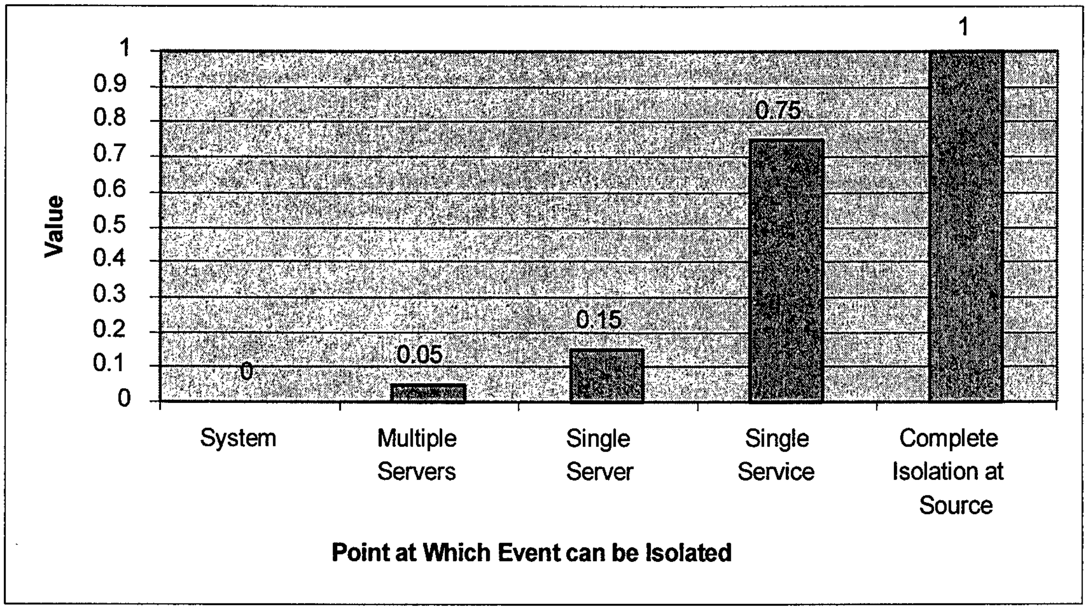
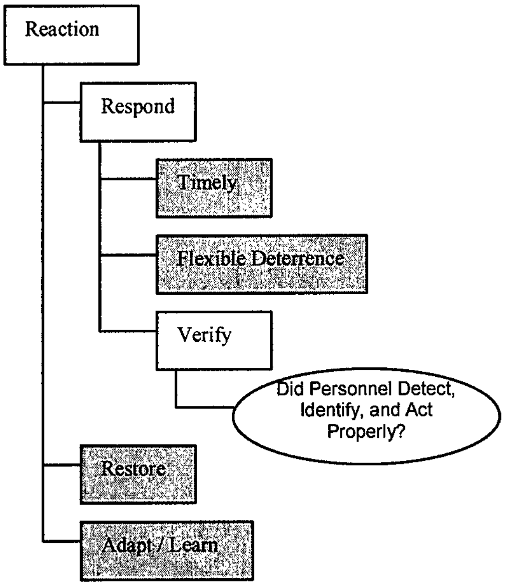


Figure A-28: Flexible Deterrence: Point at which an System can be Isolated during Event



Verify: The ability of the system or system administrators to determine, after the event, if their actions, which include detecting, classifying, and gathering evidence from an event, were appropriate.

Rationale: Decisions must be made quickly during an event. After the event is over, it is therefore necessary to determine if the decisions made were the correct decisions. For instance, after responding to an attack, the system administrators would like to have the ability to go back to system logs and see if enough information about the event was retained. If, after careful review, it was thought that a better action could have been taken, a different course of action or procedure may be necessary if a similar event occurred in the future.

Measure: After further review of the response process, did AFTAC personnel identify, categorize, and act properly given the nature of the event. The measure is a binary Yes or No, with Yes receiving a value of 1.0 and No receiving a value of 0.0. There is no middle value in Verify because it was felt that when the organization reflects upon its actions, they either detected the event, categorized it, and reacted to it correctly or they did not. Therefore personnel must accomplish all three tasks in order to receive a score of 1.0.

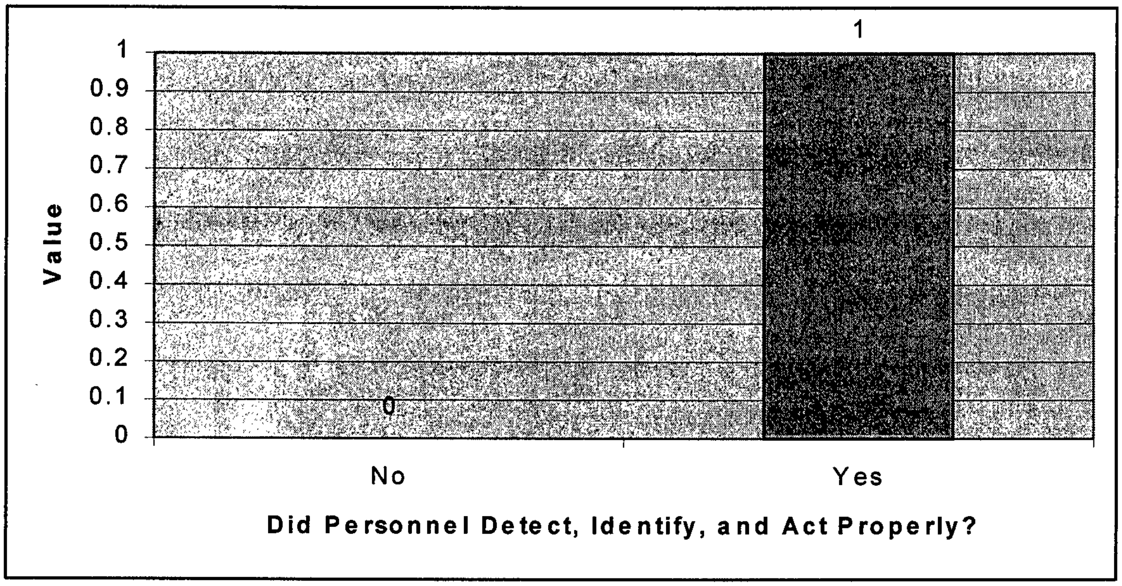


Figure A-29: Verify: Did Personnel Detect, Identify, and Act Properly?

Restore

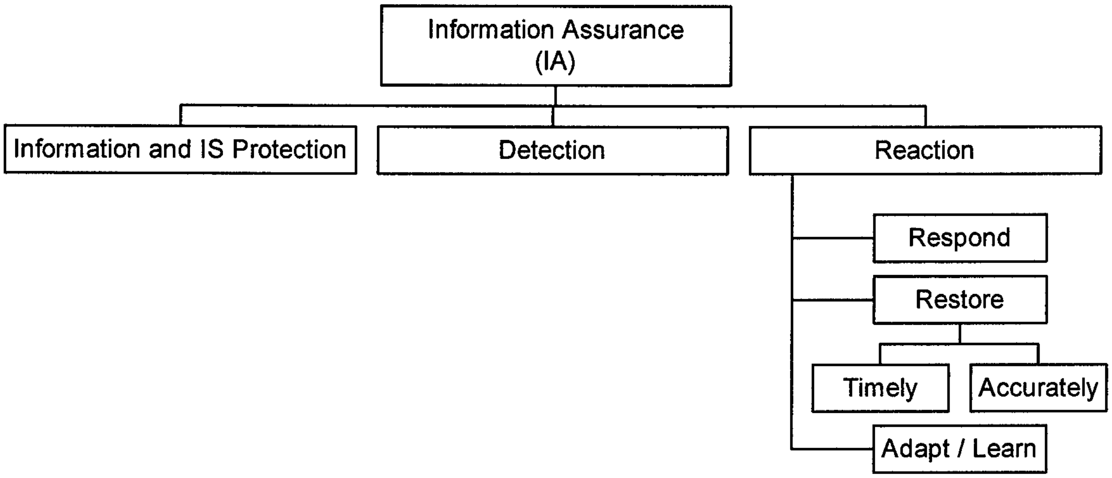


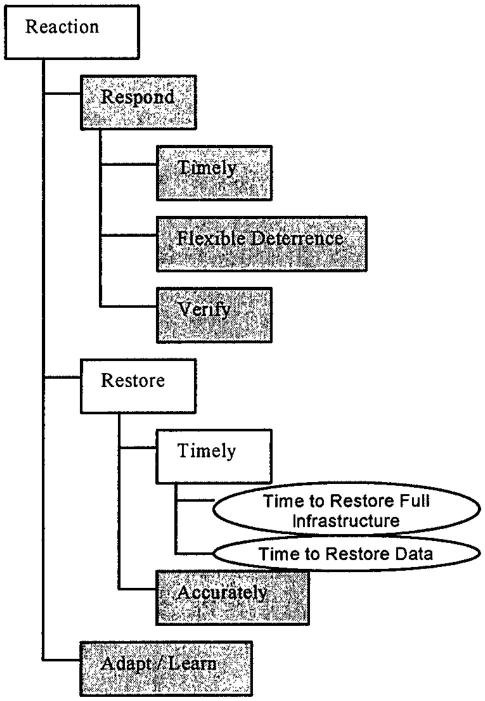
Figure A-30: Restore

Restore: The ability to restore information or an information system to an acceptable level after an event.

Rationale: Information must be restored to an acceptable state after an event. Both time and accuracy are considered when determining if the restoration was successful. The idea of graceful restoration, where systems can be brought back step by step instead of in an all or nothing fashion, is key in determining the restoration capabilities of a system.

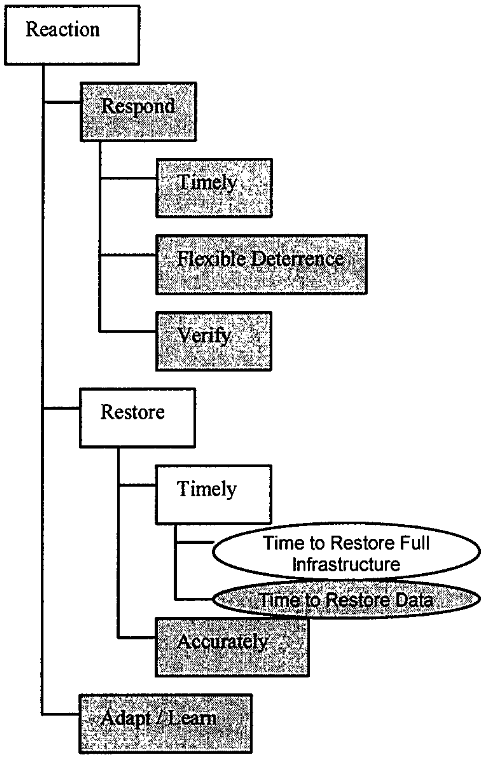
Timely: The amount of time needed to recover and restore information to an acceptable level.

Rationale: Failure to restore information in a timely manner could result in permanently lost information, prolonged vulnerability, or decreased mission capability.



Measure: Amount of time needed to restore mission capabilities. This measure is separated into two parts: the amount of time to restore full infrastructure and the amount of time to restore data. The amount of time to restore full infrastructure is measured in hours, and the amount of time to restore data is measured in days, as it often takes much longer. In addition, some missions can be accomplished when the infrastructure is restored but not all databases have been restored and verified as accurate.

Time to Restore Full Infrastructure: The amount of time needed to fully restore the system to its original capability. The faster full infrastructure can be restored the more valued it is to the organization. The curve is steeper from 0 to 2 hours because of the importance of restoring the system in under two hours. No value is gained for restoring the system after 6 hours.



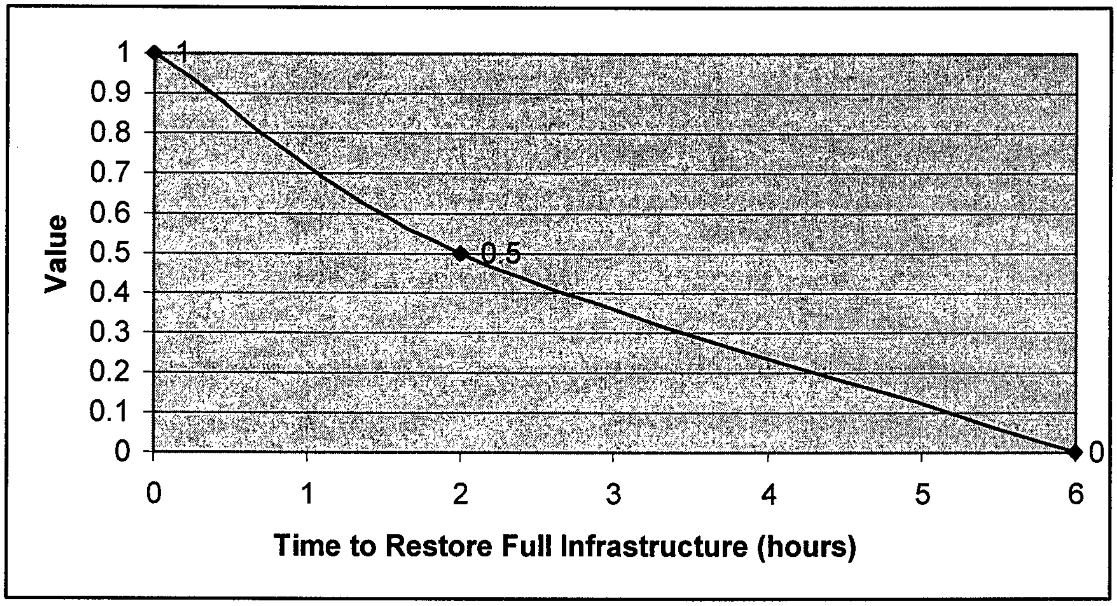
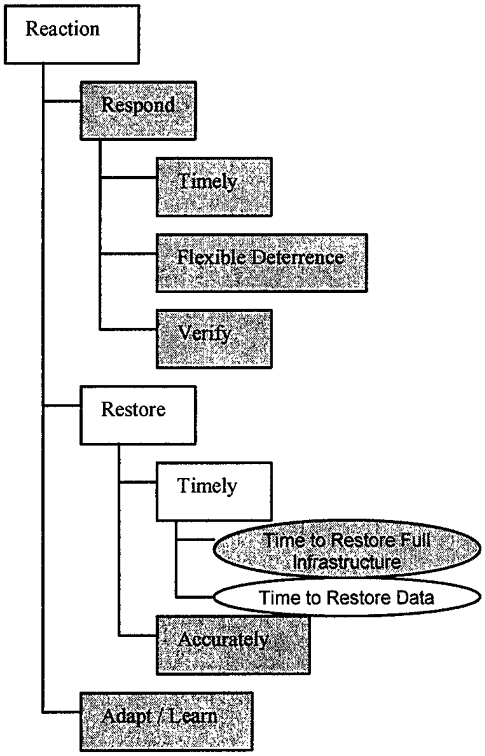


Figure A-31: Amount of time to restore full infrastructure, measured in hours

Time to Restore Data: The amount of time needed to retrieve and restore lost or damaged data to the system. This process often takes a longer period of time then infrastructure restoration since it involves the process of determining what data was lost, finding the last instant when the data was not corrupt, and restoring the system with the uncorrupted data.



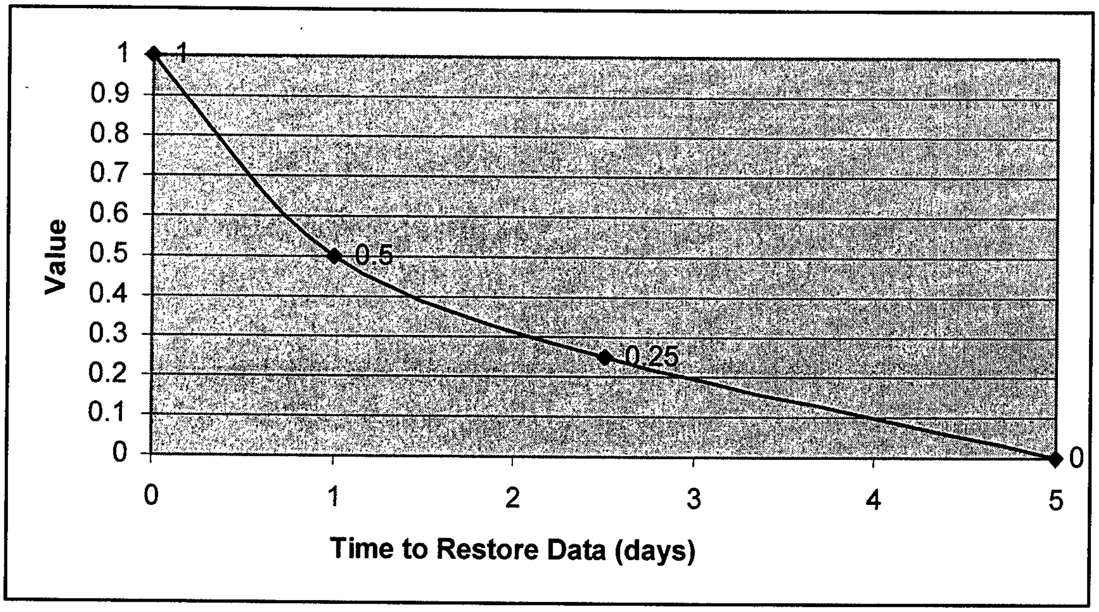
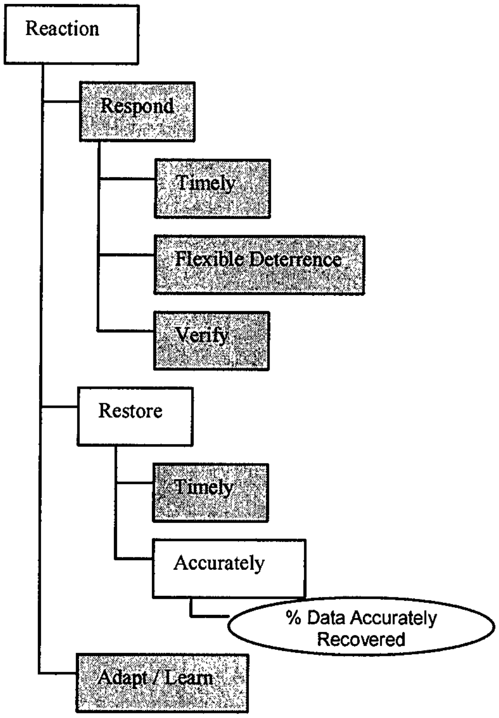


Figure A-32: Time to Restore Data, measured in days



Accurately: The information restored must be correct.

Rationale: Restoration of incorrect information is not acceptable and therefore has no value to the unit.

Measure: The percent of data accurately recovered. Again, inaccurate recovered data has no value, so only the percent of correct data recovered is considered. No value is given unless at least 20% of the lost data can be recovered. The curve rises gradually to 80% and then becomes steeper because there is little value to the unit if they cannot recover all or almost all of the lost data.

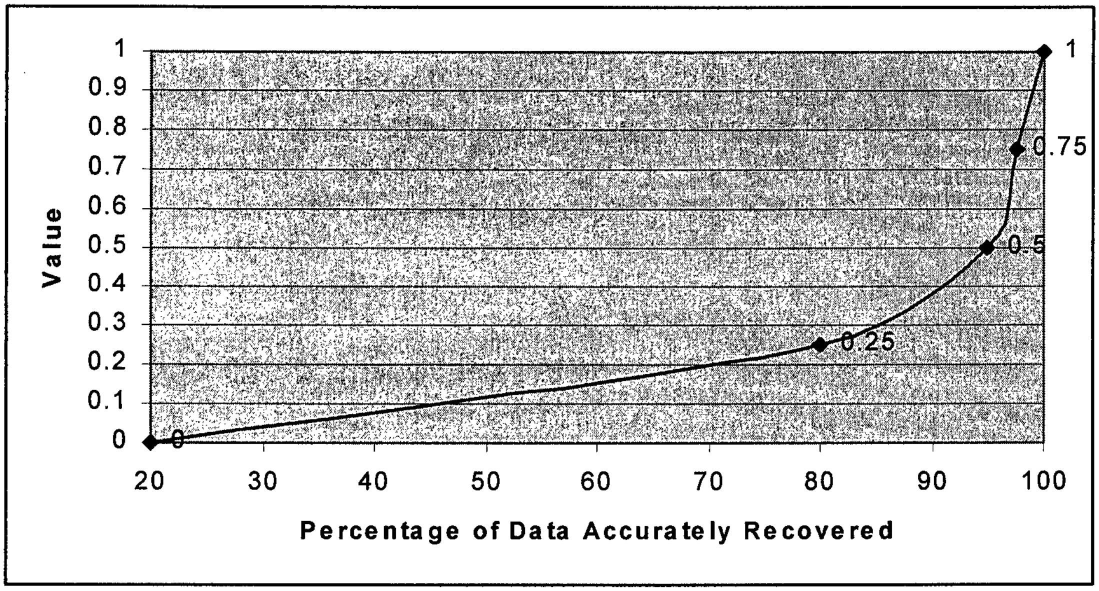
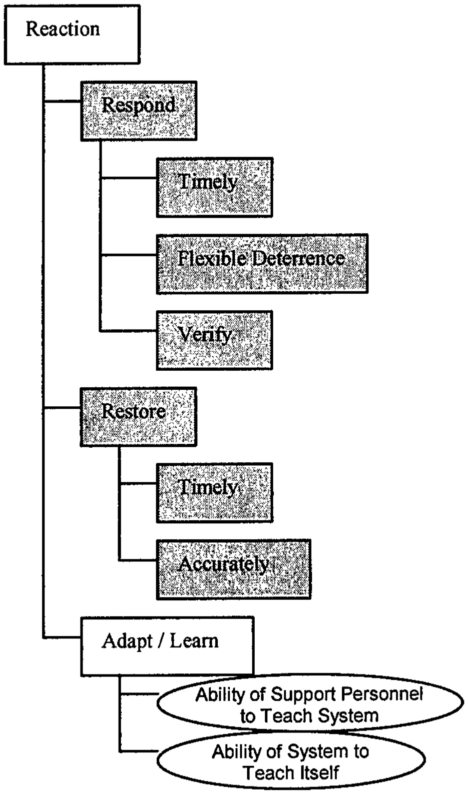


Figure A-33: Percentage of Data Accurately Recovered



Adapt / Learn: The ability of the system or system users to learn from an event and adapt to the new situations resulting from the event.

Rationale: Learning from mistakes or events and taking corrective action prevents the same errors from occurring multiple times.

Measure: This measure was separated into two parts: the ability of support personnel to teach the system, and the ability of the system to teach itself. The reason for the separation is that it is beneficial to allow personnel to manipulate system algorithms when necessary. The most desired characteristic is that the system can teach itself. When the two functions are combined, the best possible case is a system that will adapt automatically, but will allow an administrator to teach it different procedures when needed. The worst case is a system that is completely unchangeable, meaning that it does not learn from past vulnerabilities and cannot be programmed to deal with them in the future. Each separate function must be weighted to determine if the ability of support personnel to teach the system is more important than the ability of the system to teach itself, or vice versa.

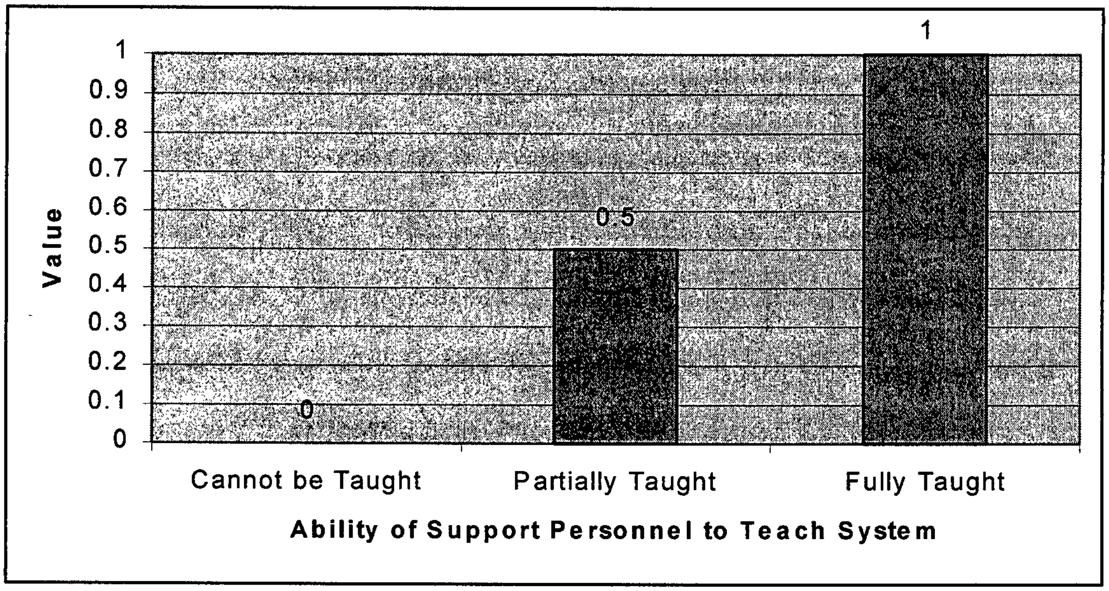


Figure A-34: Ability of Support Personnel to Teach the System

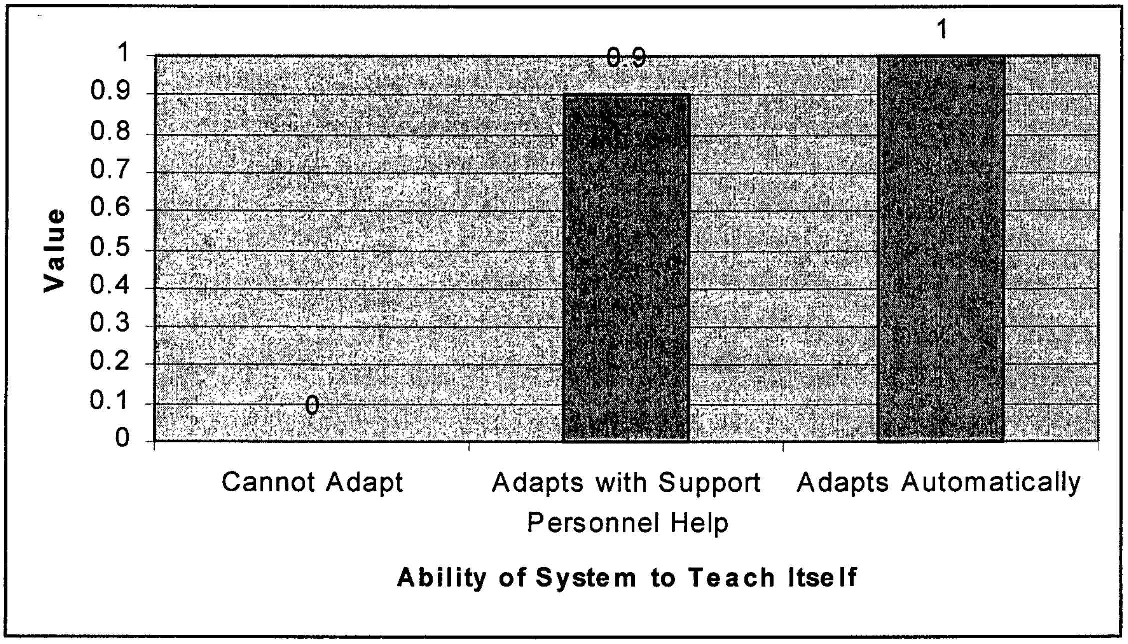


Figure A-35: Ability of System to Teach Itself

Impact of IA on System Operational Capability

Changes to information assurance are likely to impact system operational capability and therefore they must be considered in the study. The complete Impact of IA to System OC hierarchy is shown in Figure A-36.

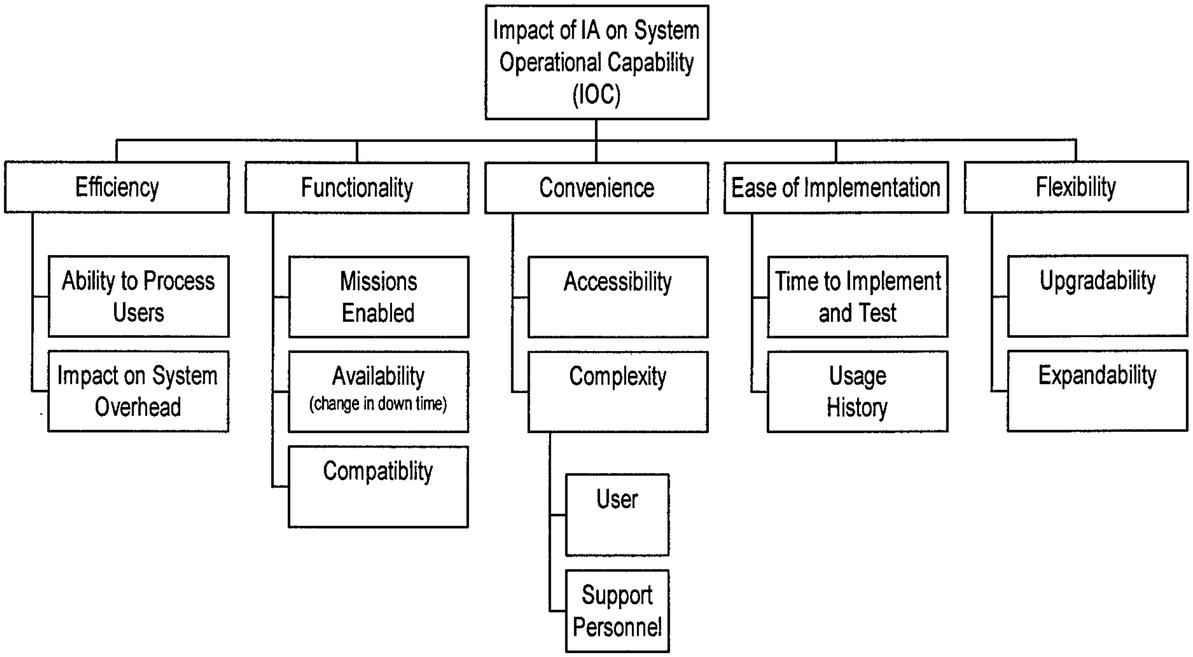


Figure A-36: Impact of Information Assurance on System Operational Capability

Impact of IA on System Capability: The amount of system operational capability (OC) gained or lost due to implementing a new IA strategy.

Rationale: Changing the system to improve IA will almost certainly have some impact on the system's operational capability. It is therefore necessary to consider OC when determining what, if any, IA course of action should be implemented. A strategy that greatly increases IA may severely reduce system operational capability and therefore may not be the best alternative when all factors are considered. The most desired goal is to improve IA and positively impact the system's operational capability, if possible.

Efficiency

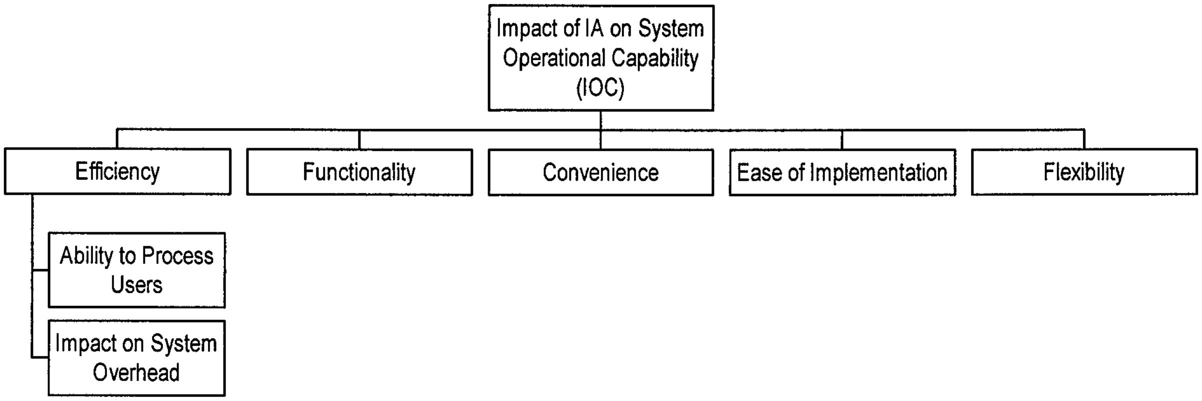
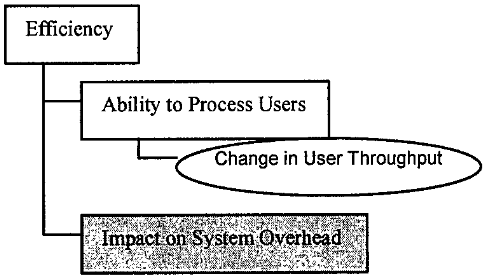


Figure A-37: Efficiency

Efficiency: The system can perform the required tasks quickly and consistently with respect to demand on the system.

Rationale: Implementing an IA strategy may impact the speed of the system, which would force it to be able to process a different amount of information per time period. This value is broken down into the Ability to Process Users and the Impact on System Overhead.



Ability to Process Users: The impact an IA strategy will have on the system speed and usage with respect to the system users (not support personnel).

Rationale: If the system is slower because of a new IA strategy, then the users may experience slower service when trying to access information. This may cause the mission to suffer since users cannot perform their jobs at the same speed as before. Likewise, an increase in user service due to an IA strategy will allow users to do their missions faster and perhaps more effectively.

Like many measures in the Impact of IA to System OC hierarchy, this measure focuses on the *change* the IA strategy will have on OC. In this case, No Change is valued greater than 0.5 because most IA strategies actually decrease OC. When a strategy does not materially adversely impact the system OC, then it will usually receive a fairly high value.

Measure: The Ability to Process Users is measured by the Change in User Throughput to the system. User Throughput is defined to be the speed at which the system allows the user to work. For this measure, increasing user throughput at all will gain a value of 0.85. Again, this is due to the fact that any increase in OC from an IA strategy is a welcome bonus.

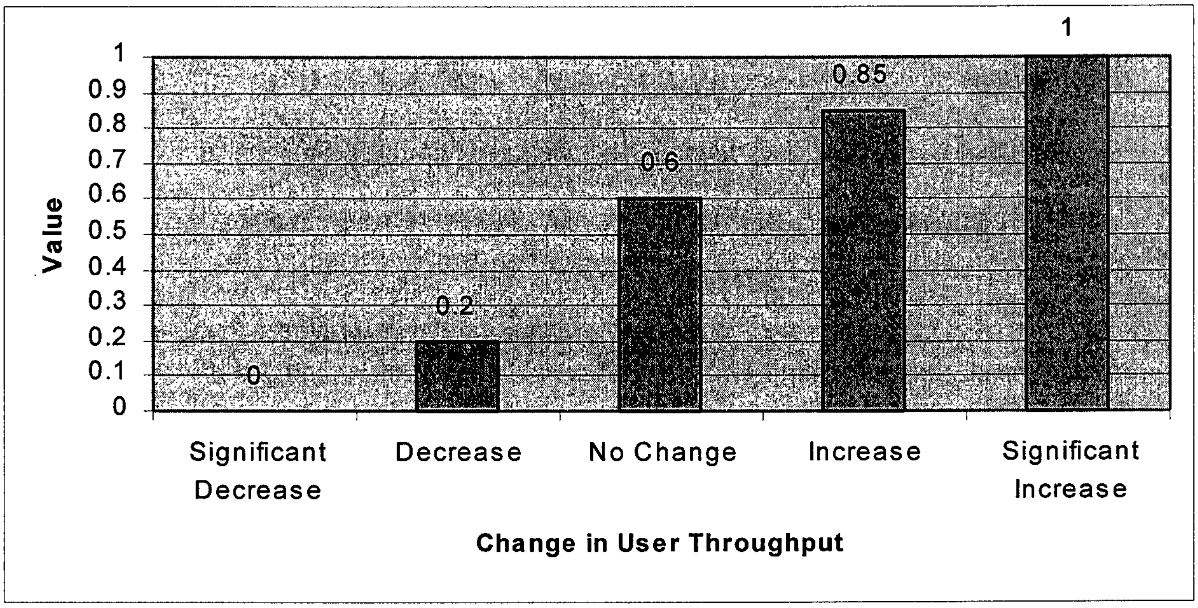
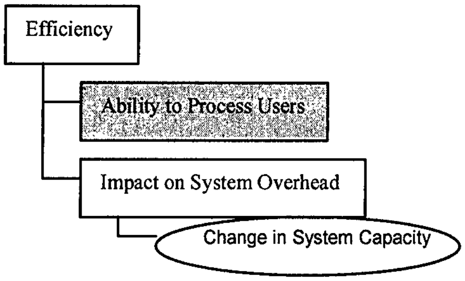


Figure A-38: Ability to Process Users, measured as the Change in User Throughput

Impact on System Overhead: The percent capacity of the system an IA strategy requires.



Rationale: The less an IA strategy negatively impacts system capacity the better the strategy will be (all other things being equal). A system running at 80% capacity will be less effective then a system running at 50% capacity assuming both can do all jobs equally. Increasing a two-lane highway into a four-lane highway will increase the capacity of the road, thereby making its ability to process automobiles more efficient (more cars can now use the highway then before). Likewise, an IA strategy that allows more information to be processed will increase the system capacity, and therefore the system operational capability.

Measure: Impact on System Overhead is measured by the change in system capacity due to an IA strategy. Again, no change to the current system is seen as a good alternative, scoring a 0.6. Increasing system capacity scores a 0.85, but decreasing capacity scores a 0.2.

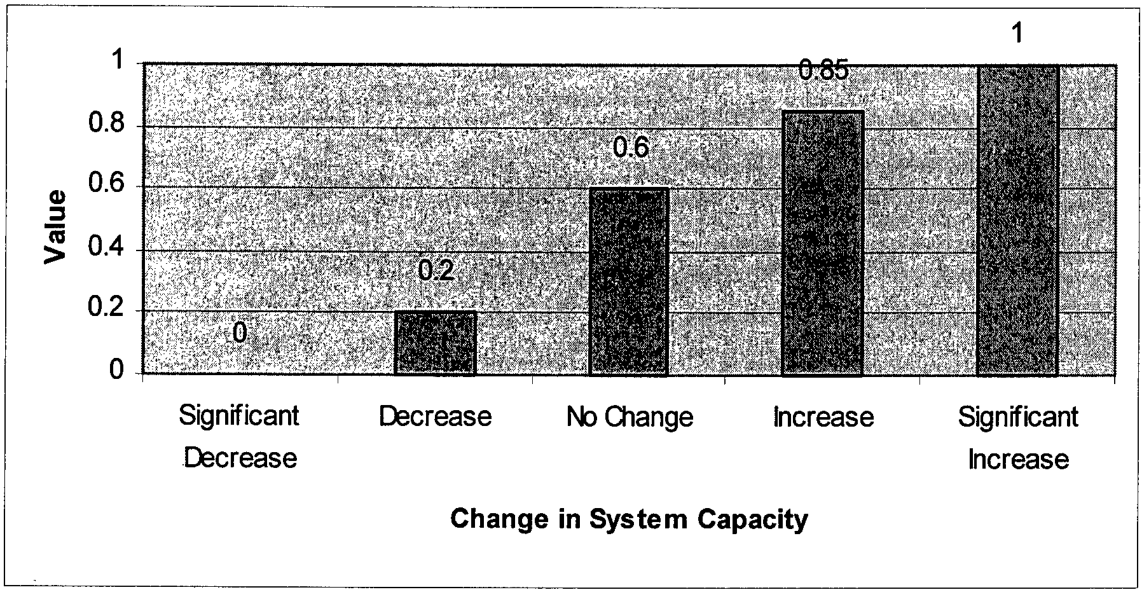


Figure A-39: The Impact on System Overhead, measured as the Change in System Capacity

Functionality

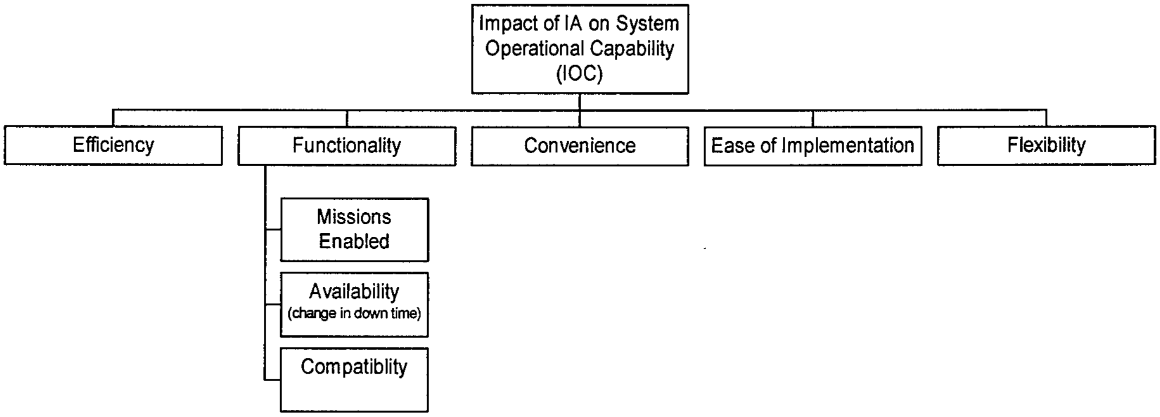
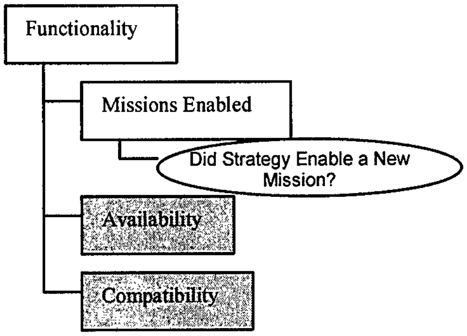


Figure A-40: Functionality

Functionality: The usefulness offered to system clients by providing information and information related capabilities (both desired and essential)

Rationale: A change is the system usefulness (in relation to the mission or the users) will affect system functionality. For example, if a new IA strategy allows the system to perform a new function, then the overall usefulness of the system increased. Likewise, if a strategy now forces the system to be down 50% or more of the time than it used to be, the system has lost functionality because its users cannot access the system. This value was separated into Missions Enabled, Availability, and Compatibility.

Missions Enabled: Did the new IA strategy allow the system to perform any new missions or functions?



Rationale: It was determined through discussion that no IA strategy that removed a mission would ever be considered for implementation on the target system. Therefore only the ability to add new missions or functions to an existing system will be considered.

Measure: The measure is simply determining if the new IA strategy enabled the system to perform more missions or functions than it previously could.

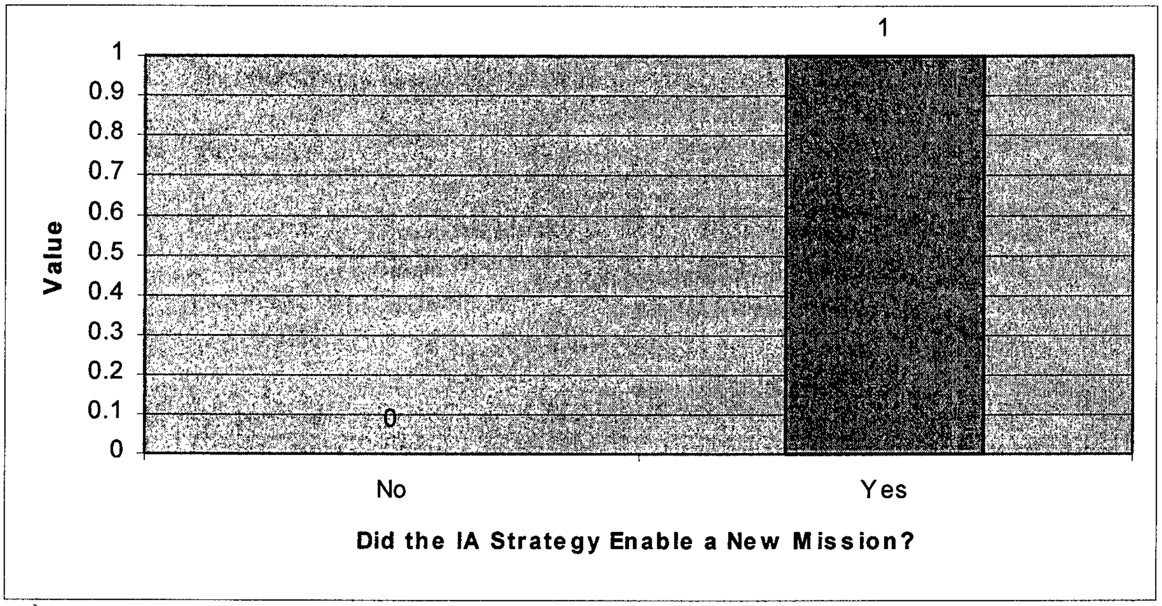
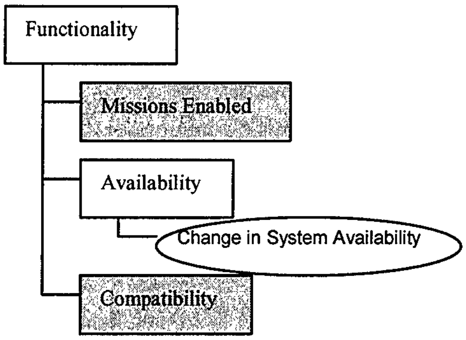


Figure A-40: Missions Enabled, measured as the Ability of the IA Strategy to Enable New Missions



Availability: The change in downtime due to an IA strategy.

Rationale: A system that is down too much will decrease mission performance. If an IA strategy causes the system to be down five times a week (compared to say three times before the new strategy), then the system has lost availability and thus functionality.

Measure: The Change in System Availability is used to measure how the new IA strategy affects previous system availability. Availability is crucial to mission accomplishment, thus No Change scores a 0.9. Figure A-41 shows that while increasing availability might be nice, decreasing availability, even slightly, is simply unacceptable.

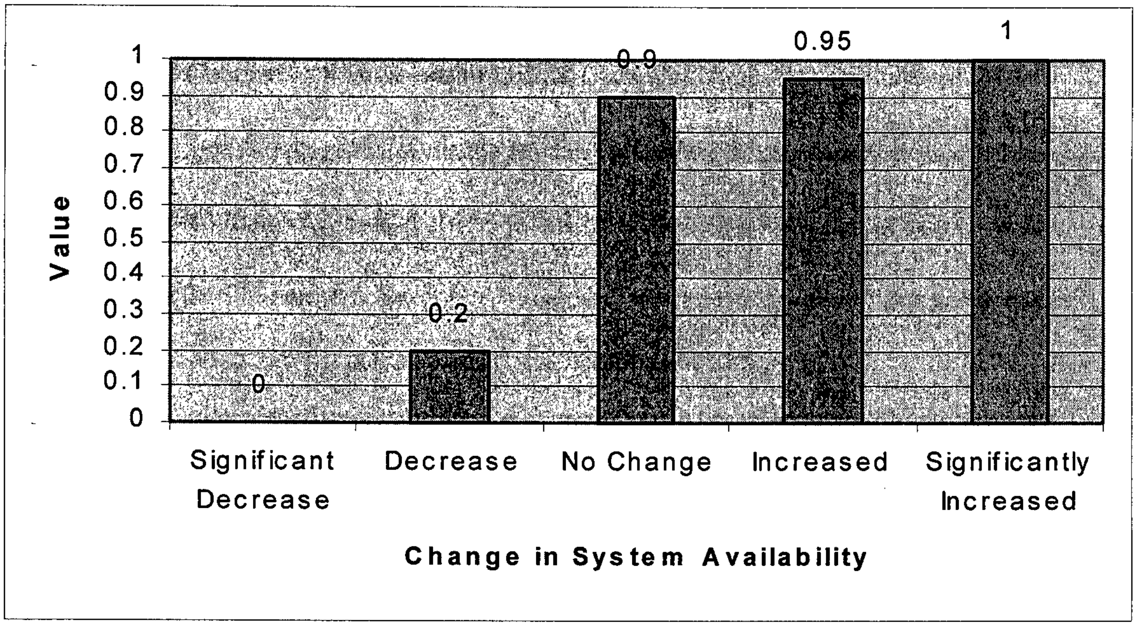
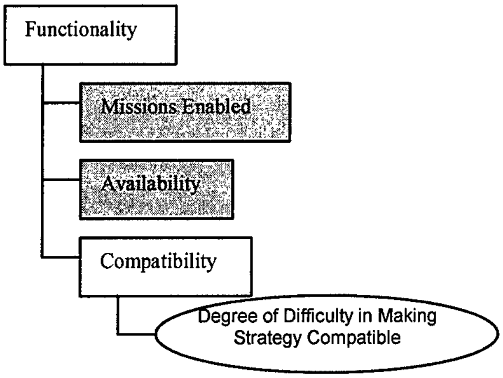


Figure A-41: Availability, measured as the Change in System Availability due to implementing a new IA strategy

Compatibility: The ability of the information system to interact with other systems, hardware, and software.



Rationale: Increasing or decreasing the amount of systems that are compatible with the current configuration could impact the usefulness of the information system. It was determined through discussion that an IA strategy that was truly incompatible would never be considered for implementation.

Measure: The Degree of Difficulty in Making a New IA Strategy Compatible is used to measure how well an IA strategy interacts with other systems. AFTAC experts agreed that almost any IA strategy can be made compatible; however some take a considerable amount of effort and some do not. The categories range from complex, where system experts spend many days working the strategy into the existing system, to strategies that involve no difficulty whatsoever, such as changing a software package from version 2.0 to version 2.5.

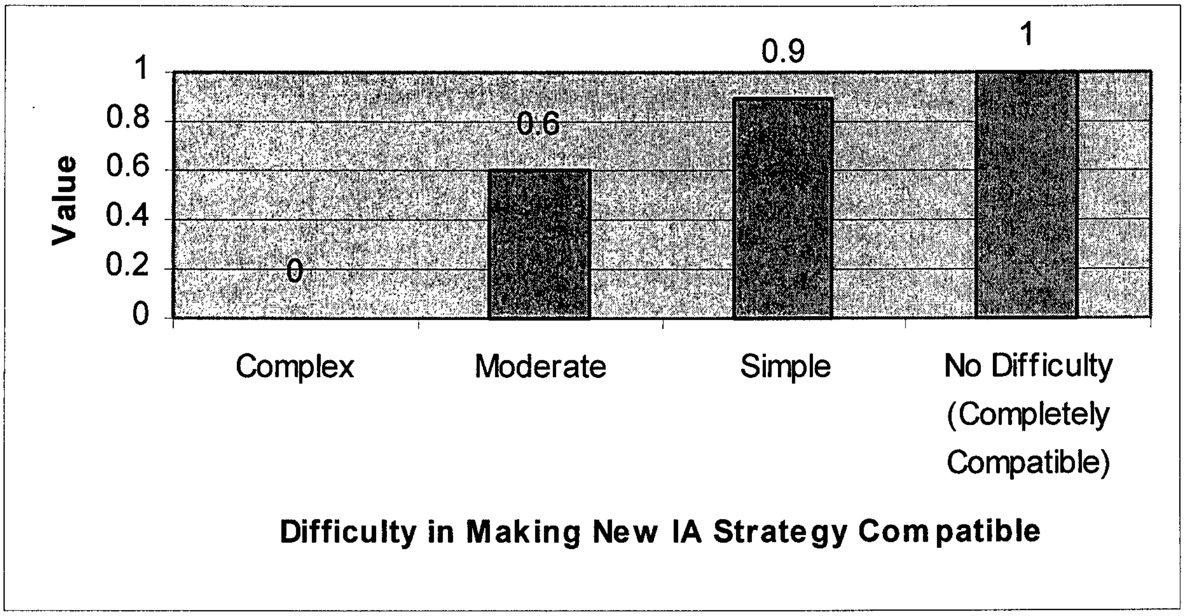


Figure A-42: Compatibility, measured as the Difficulty in Making New IA strategies Compatible with existing system configurations

Convenience

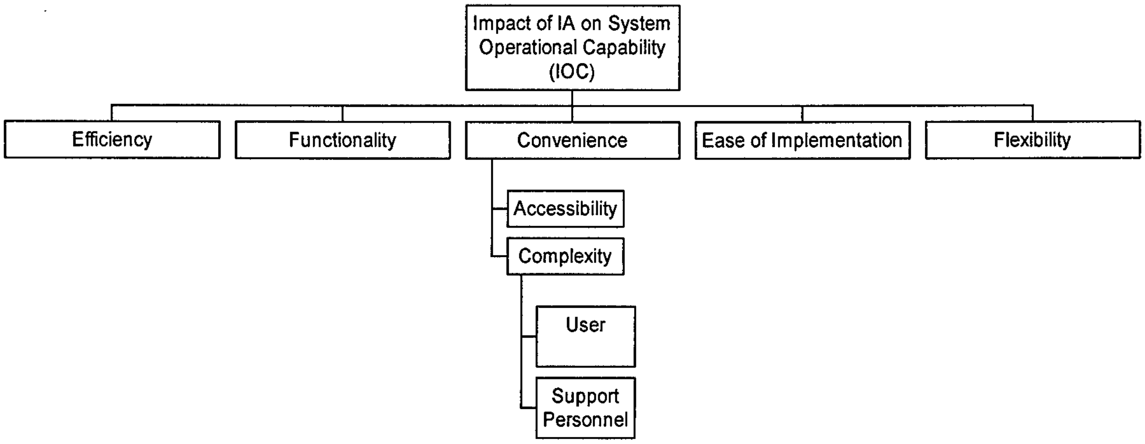
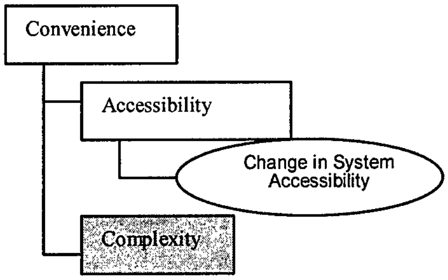


Figure A-43: Convenience

Convenience: The level of complexity needed to operate the system

Rationale: Changing the difficulty in using the system could impact how well the user is able to process information, thereby affecting system operational capabilities. A user is likely to avoid very inconvenient systems if the mission can be accomplished elsewhere or it is non-essential. The system exists to serve the users, minimize their difficulty, and provide secure, assured access to important information. Since Convenience captures the ability to access the system, and once in the system, the ability to use it, Convenience is separated into Accessibility and Complexity.



Accessibility: The change in system accessibility faced by the user due to an IA strategy.

Rationale: Changing the user's ability to gain access to the system could cause the user to waste valuable mission time just trying to logon to the system. Likewise, a user may be able to gain access more quickly due to an IA strategy, such as using a smart card.

Measure: Accessibility is measured by the Change in System Accessibility. This graph contains more categories than previous graphs because of the sensitivity of system accessibility; very small changes can have a large impact on the ability of a person to use the system. A score of No Change gains the strategy a score of 0.5, meaning that this is a neutral position. The magnitude of value difference on either side of No Change is the same regardless of whether accessibility was increased or decreased.

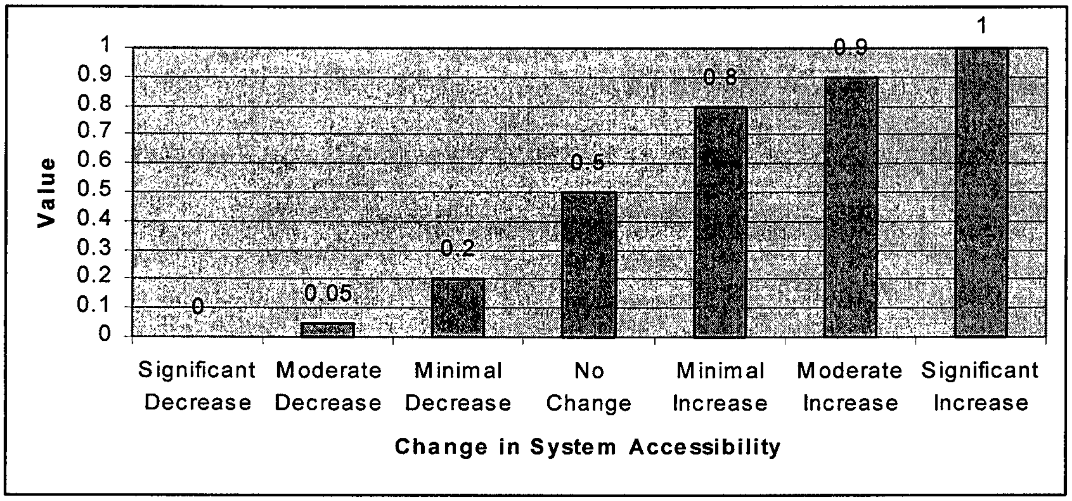


Figure A-44: Accessibility, measured as the Change in System Accessibility

Complexity

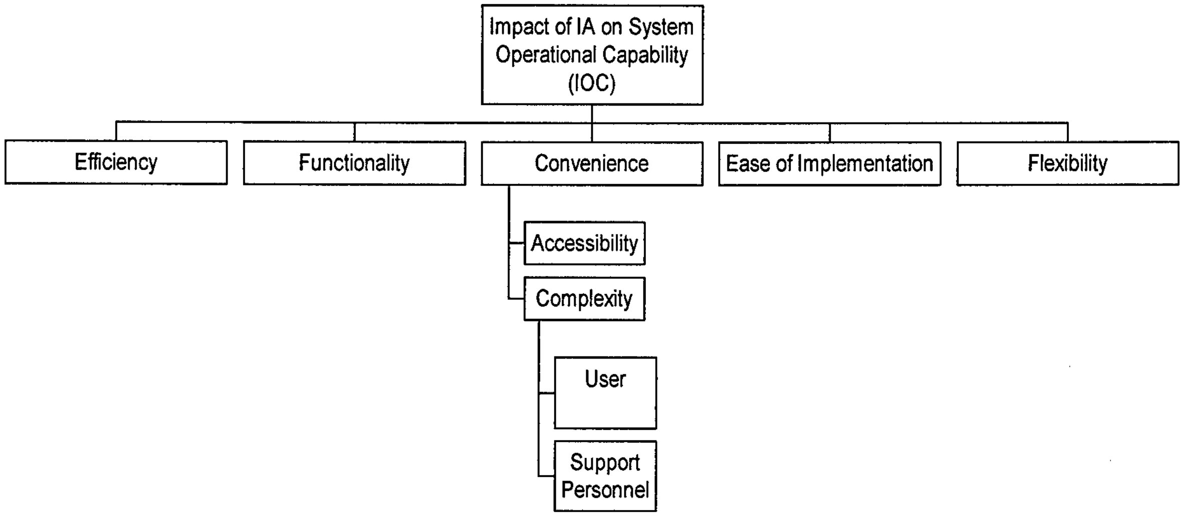
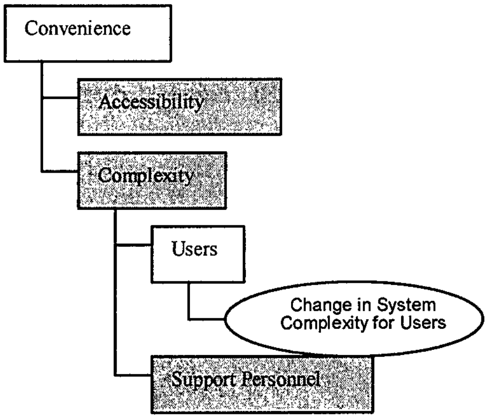


Figure A-45: Complexity

Complexity: The level of difficulty in using the system, both for users and support personnel.

Rationale: The longer it takes to train and become proficient in a system, the less time that person has for performing their mission. Since this differs for users and support personnel, they are treated separately. AFTAC support personnel feel that the systems are there to help the users perform the mission, and support personnel must ensure the systems are useable. Therefore it was deemed by support personnel in the study that it was far better to have a system that is easy for users to work, yet difficult for support personnel to maintain, than it would be if the situation were reversed.

Users: The complexity of training and using the system on the user end.



Measure: Again, this value is measured relative to the original system. Not changing the degree of difficulty in using the system scores a 0.5. Making a system more complex to the users will cause a loss in value while making it less complex for users results in a gain in value.

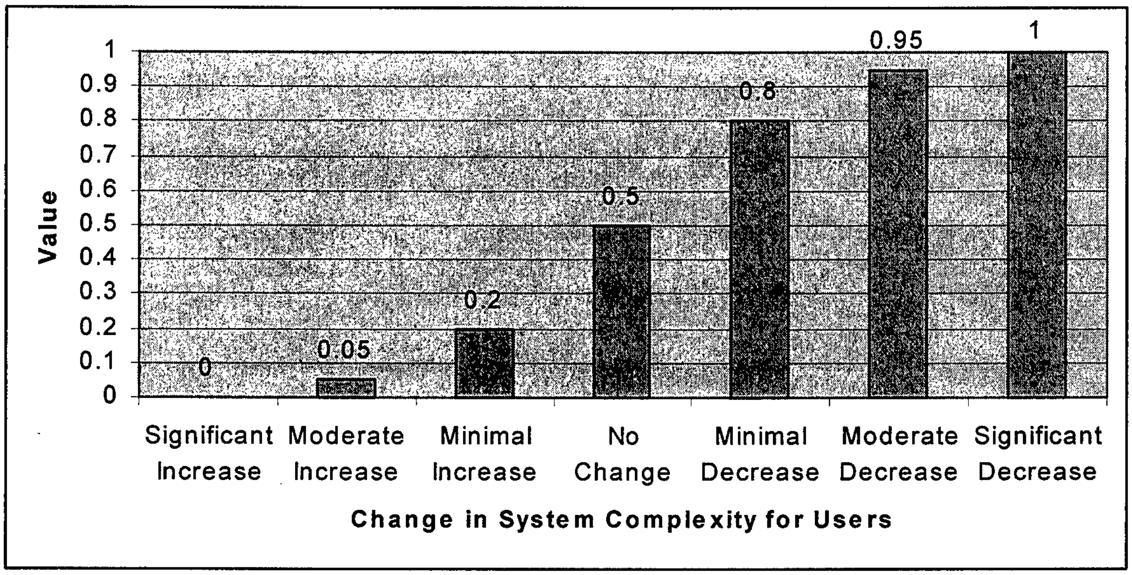
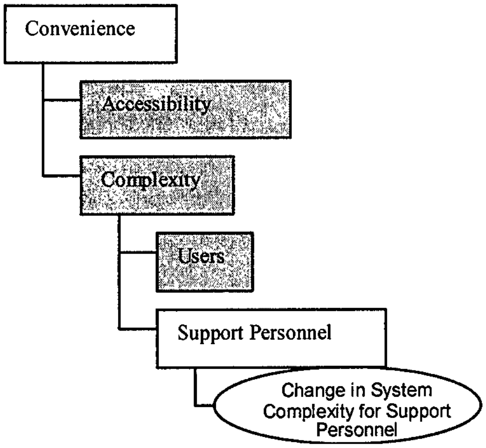


Figure A-46: User Complexity, measured as the Change in System Complexity for Users



Support Personnel: Complexity of training and using the system for support personnel. Support personnel are defined as any person responsible for system upkeep.

Measure: This value is measured using the same categories that were used for the Degree in Change in User Complexity. However, from the graph it is apparent that support personnel do not score as great a loss in value score for increasing complexity as the user graph did. As mentioned above, this is due to the fact that support personnel are willing to use a complex system themselves in order to prevent users from working on a more complex system. Support personnel do value the ability of an IA strategy to decrease complexity. The No Change category actually scores higher in this graph (0.6) than it did in the previous graph (0.5) because the support personnel in the study feel that there is better than average value to any strategy that does not make their job harder.

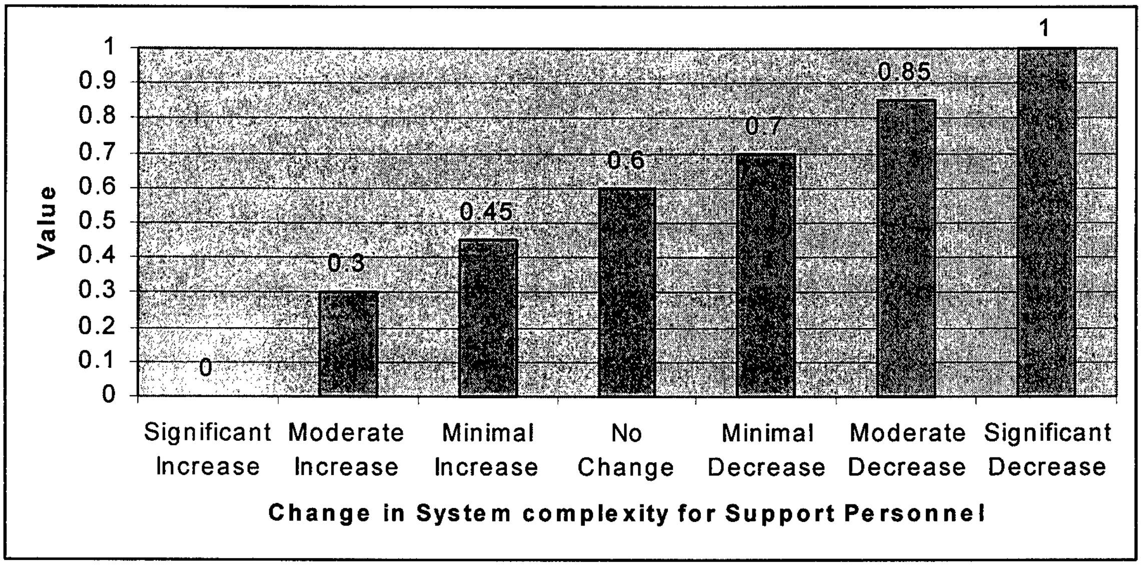


Figure A-47: Support Personnel Complexity, measured as the Change in System Complexity for Support Personnel

Ease of Implementation

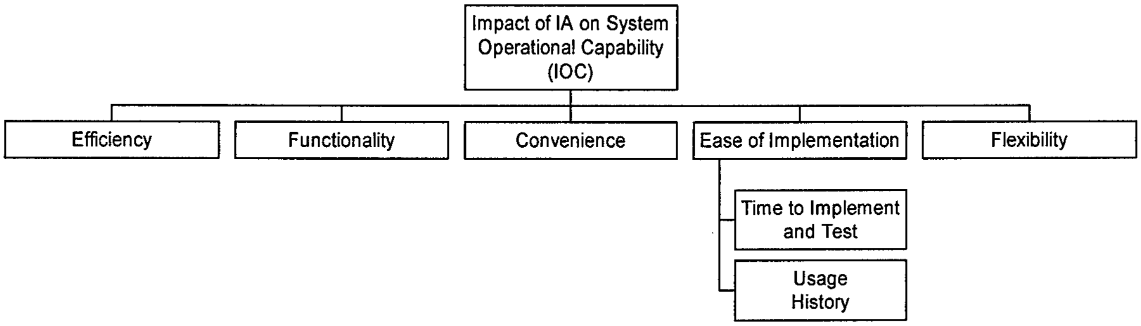
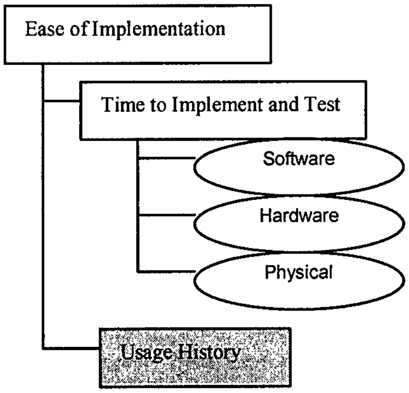


Figure A-48: Ease of Implementation

Ease of Implementation: The degree of difficulty associated with installing a new IA strategy

Rationale: An IA strategy that is very difficult to implement may impact system OC due to time, training, and testing. Ease of Implementation was separated into the Time to Implement and Test and Usage history.



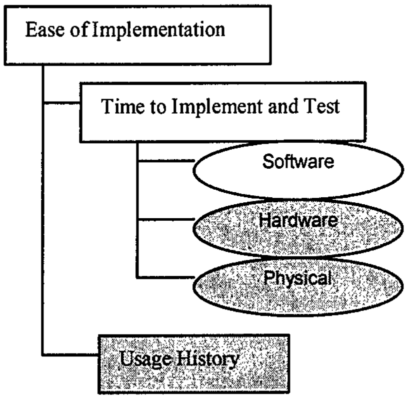
Time to Implement and Test: The time needed to implement and test an IA strategy.

Rationale: It is important to implement and test an IA strategy in a timely fashion.

Measure: This value is separated into three categories: the time it takes to implement software strategies, hardware strategies, and physical strategies. This separation was used because of the relative time to implement is valued differently for each type of strategy. For example, if what is believed to be a simple software upgrade ends up taking all day to install, then it would receive no value.

However, a physical information assurance measure that can be implemented in less than one workday would receive a score of almost 1.0.

Software: The Time to Implement and Test Software strategies is measured in hours since these types of installations usually occur within one workday. The graph shows that there is a significant value drop after three hours. After four hours, the curve becomes even steeper, and anything over six hours is seen as a significant burden and receives no value.



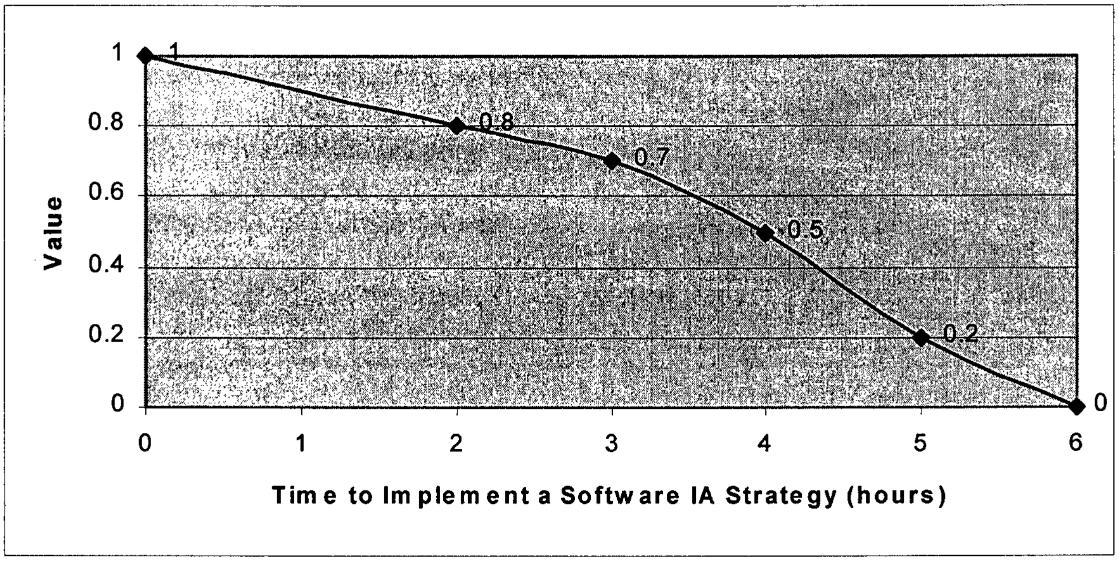
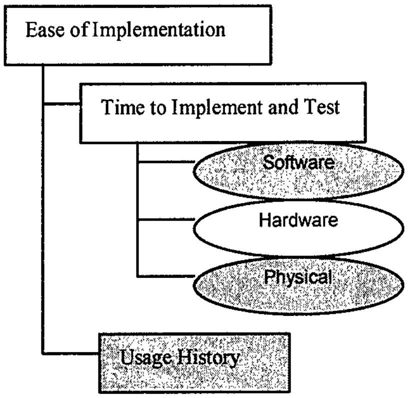


Figure A-49: Time to Implement and Test a Software IA Strategy, measured in hours



Hardware: Hardware implementations typically take longer to accomplish than software installations, thus it is measured in workdays. Very high value is given for installations that take less than half a day. After a half-day, the curve is steep to one-day implementation time. After one day, the curve is somewhat linear with a few minor slope adjustments until it reaches the value endpoint of six workdays.

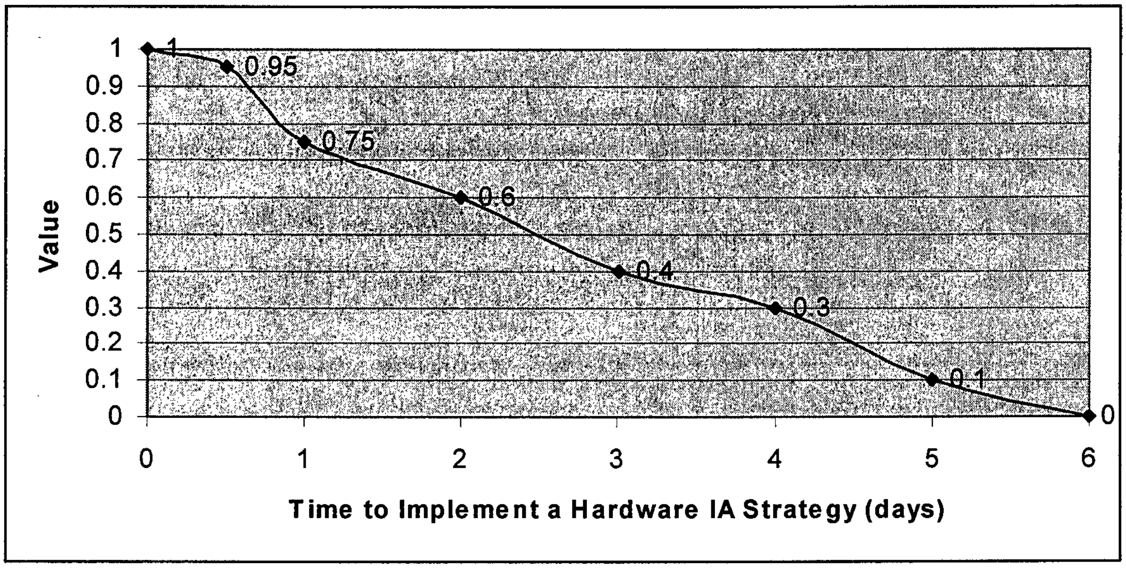
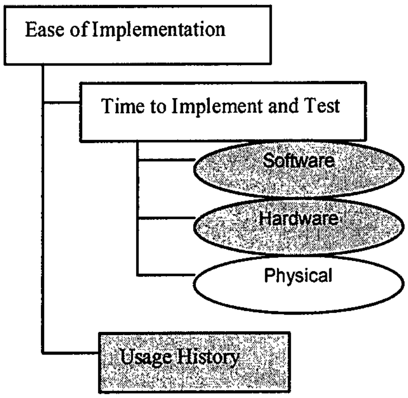


Figure A-50: Time to Implement and Test a Hardware IA Strategy, measured in workdays



Physical: Physical IA strategies tend to take even longer than hardware implementations, and therefore physical implementations are measured in workweeks. If the task can be accomplished in under a week then at least 80% of the value will be earned. Tasking taking four weeks (about one months' time) or more receive no value for this measure. Many physical strategies inconvenience users and support personnel due to construction, crowded office space, deliveries, and so forth. Therefore the value drop from week to week increases until the third work week, where almost all value is lost.

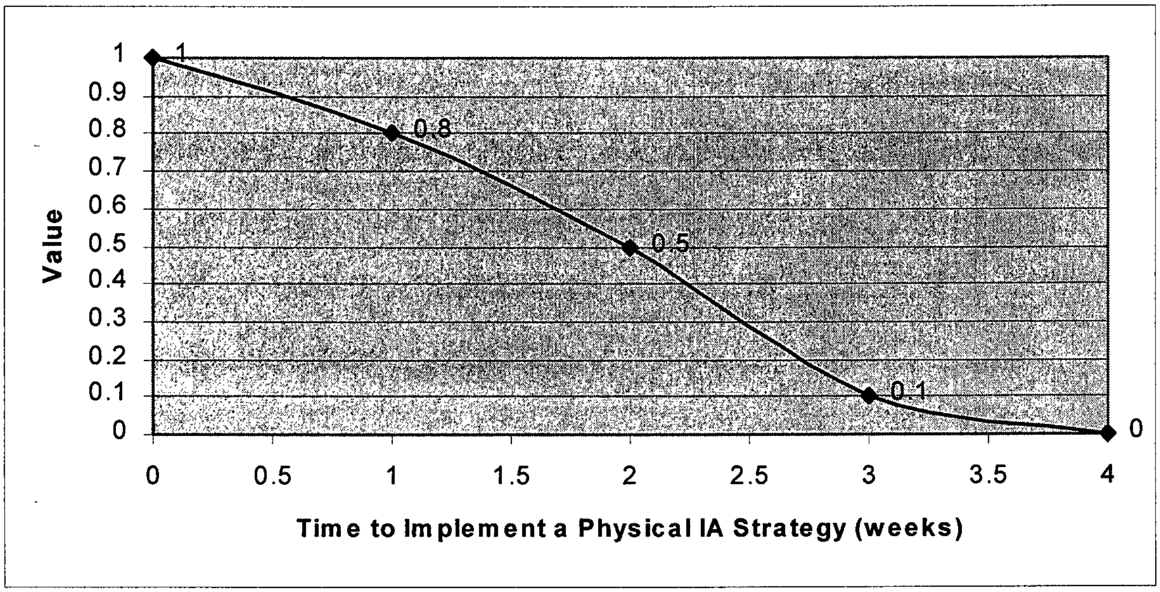
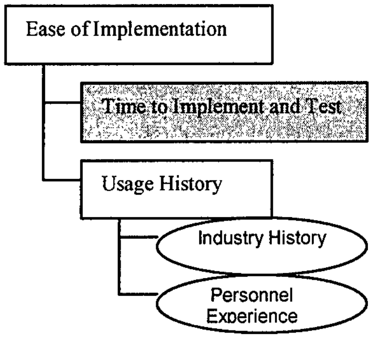


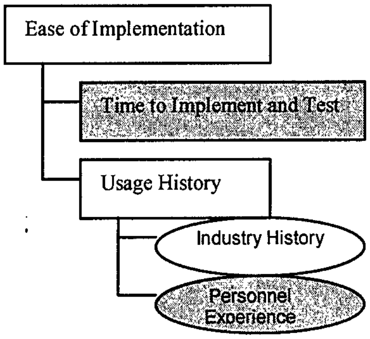
Figure A-51: Time to Implement and Test a Physical IA Strategy, measured in workweeks



Usage History: The track record of a hardware or software IA strategy; i.e. how the product fared in the past, particularly on similar systems.

Rationale: It was considered better to use hardware or software that has been proven to be operationally effective compared to items that are absolutely brand new and may have errors that might not yet have been discovered. There is some trade-off between using state of the art but untested products and highly reliable products that have been previously tested.

Measure: This measure was separated into two parts: the history of the strategy across industry and the unit personnel's experience with that strategy. While a strategy might be common practice in industry, if no one in the office had ever used it before then it might not be the best alternative for the organization. On the other hand, if a strategy is not the industry standard but AFTAC personnel have a depth of experience with it, the strategy would be favored in the second measure although not the first. Industry usage and unit experience are both valued.



Industry History: This measure is capturing how well the product has fared in similar situations over time. An industry standard is a product that is widely used and widely accepted by similar organizations and / or information systems. This also means that help is readily available from outside sources should AFTAC need it. No Exposure means that the strategy is unique to the organization; there is no one else outside the organization that uses or has used the product.

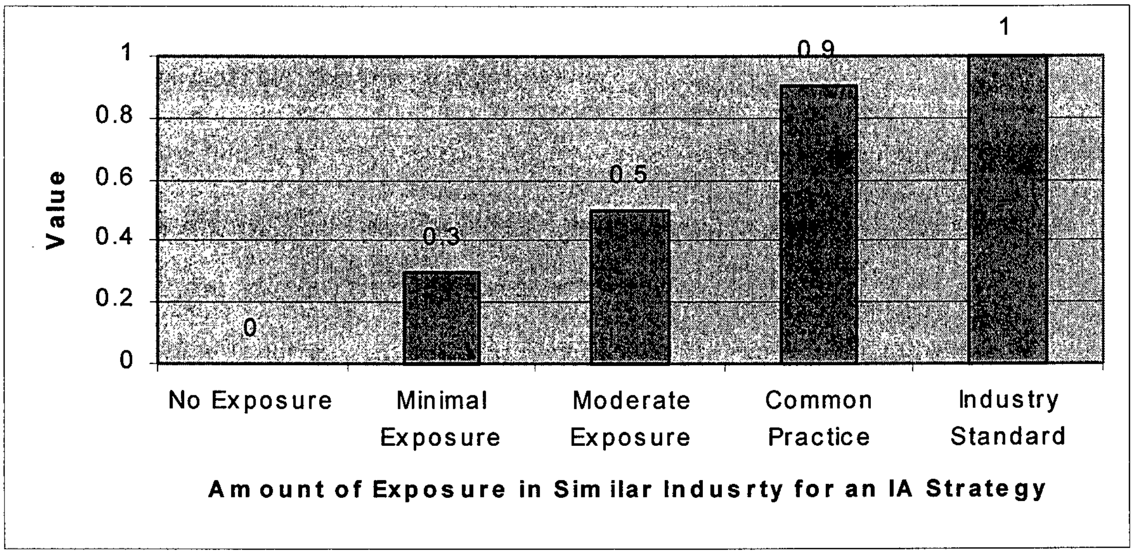
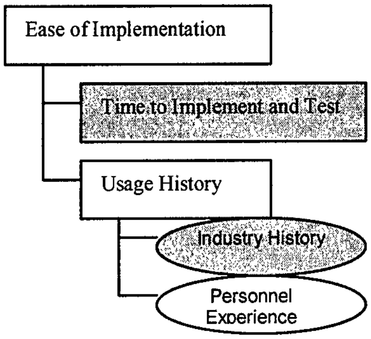


Figure A-52: Product Usage History, measured as the Amount of Exposure the Product has Seen in Similar Industries

Personnel Experience: A product's usefulness is limited if personnel at the organization have limited experience or would require numerous hours of training in order to be proficient with the product. Therefore, all other things being equal, an organization would want strategies for which its people already have expertise using. These categories are organization wide, and not necessarily the level of expertise of the highest individual. Therefore it would depend on the organization and specific strategy being considered to determine the overall personnel expertise. One person within the organization who is experienced in a strategy is better than none, but it is preferred to have wide experience throughout the organization.



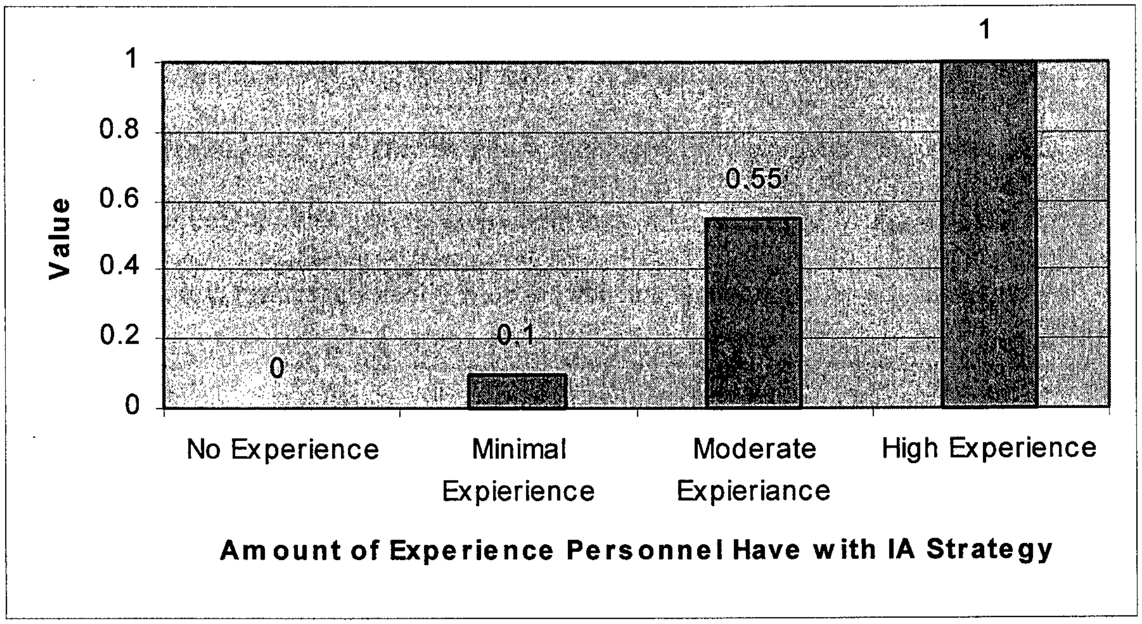


Figure A-53: Personnel Usage History, measured as the Amount of Experience Personnel have with the Product

Flexibility

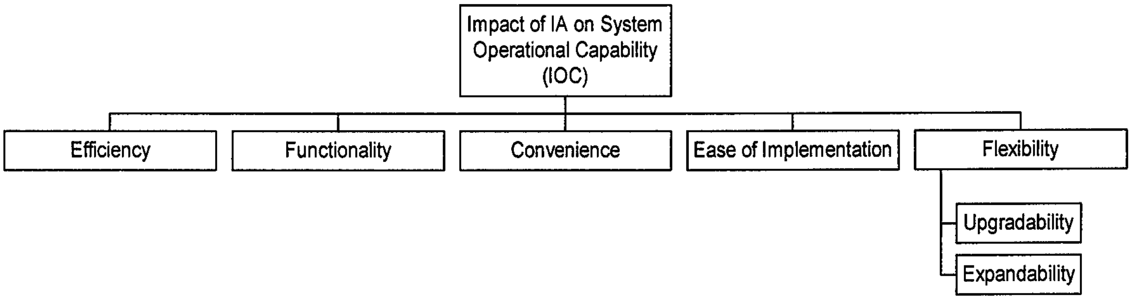
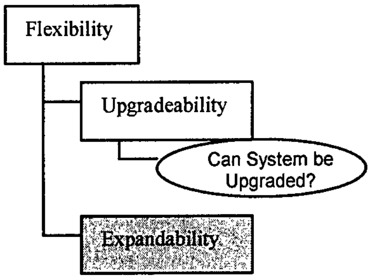


Figure A-54: Flexibility

Flexibility: The ability of the system to change over time as technology evolves.

Rationale: It is important that systems can be upgraded or expanded when new technology becomes available or the opportunity to improve the system exists. This value category is separated into Upgradeability and Expandability.



Upgradeability: The ability of the system to allow software or hardware upgrades. An upgrade involves enhancing an old product with a technologically superior one.

Rationale: Upgrades to the hardware or software due to an IA strategy may improve system performance, thereby increasing OC. It is important to note the difference between upgradeable and replaceable; almost any system can be entirely replaced once a superior one is available. An upgradeable system is one where components of the system may be changed without having to replace the entire system. For example, installing a new operating system, which also has better protection for office personal computers, would be considered a software upgrade.

Measure: After much discussion, it was determined that a strategy is either upgradeable or not, and that there is no degree to upgradeability. If a system is upgradeable, then IA experts begin to ask other questions such as whether or not it is compatible, easy to use, and so forth. System expertise will be a key consideration in the scoring of this measure.

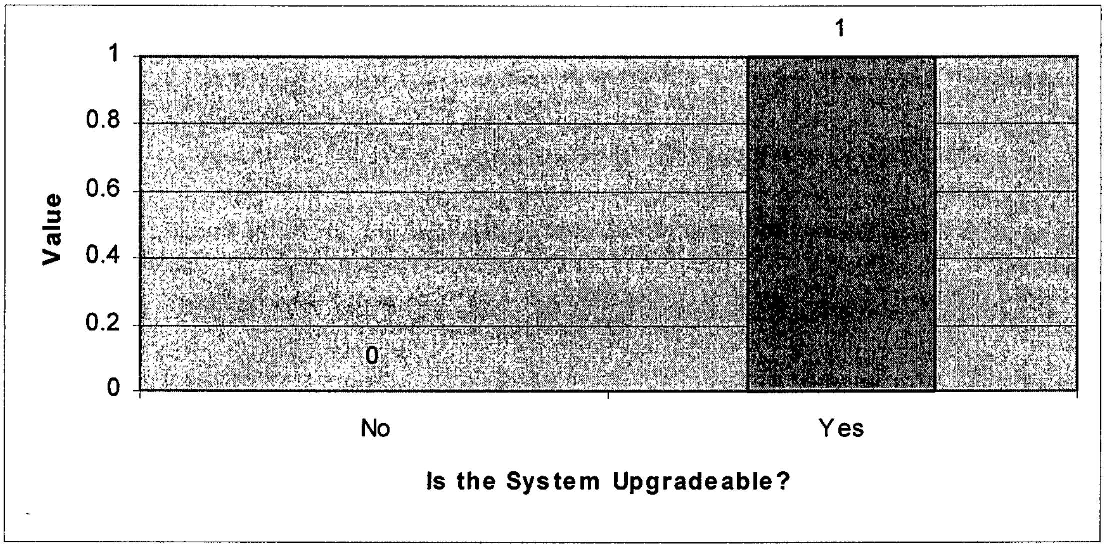
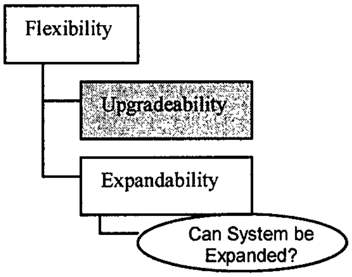


Figure A-55: Upgradeability, measured as whether or not the system can be upgraded

Expandability: The ability of the system to accept additional components. The difference between expandability and upgradeability is that expandability considers only adding similar components to a system architecture.



Rationale: A system that has the ability to expand can become more powerful without too much disruption to the system. For example, a system configuration which allows new hard drives to be easily added is more valuable then a system that needs to be completely re-configured to install the drives.

Measure: Like Upgradeability, Expandability is a binary category. A system or strategy is either expandable or it is not. Again, if the system is expandable, other qualities may be pursued, but the degree of expandability is not a factor.

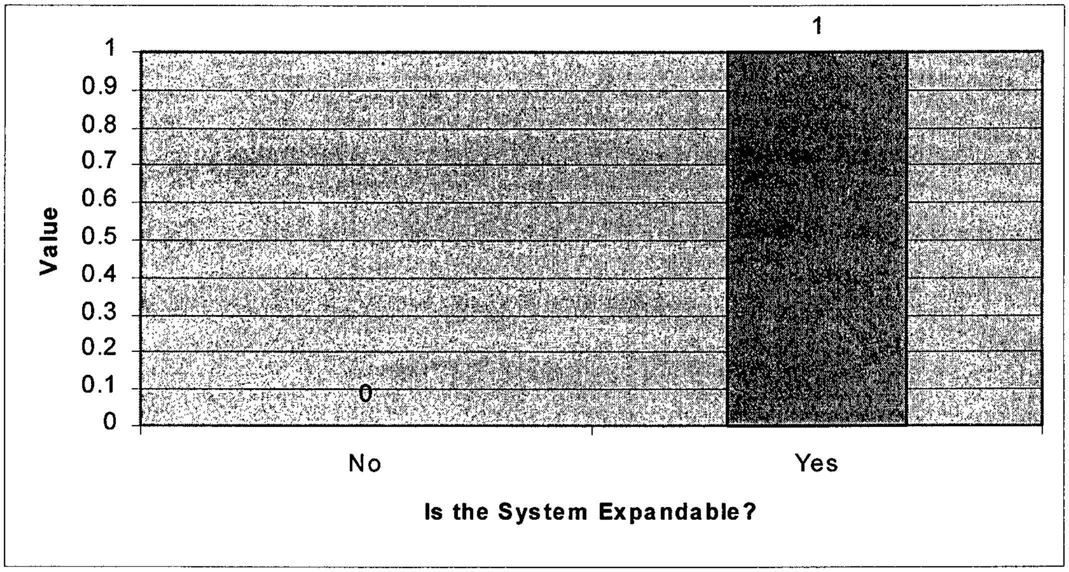


Figure A-56: Expandability, measured as whether or not the system can be expanded

Impact of IA on Resource Costs

The final sub-hierarchy, the Impact of IA on Resource Costs (IRC), is shown in Figure A-57:

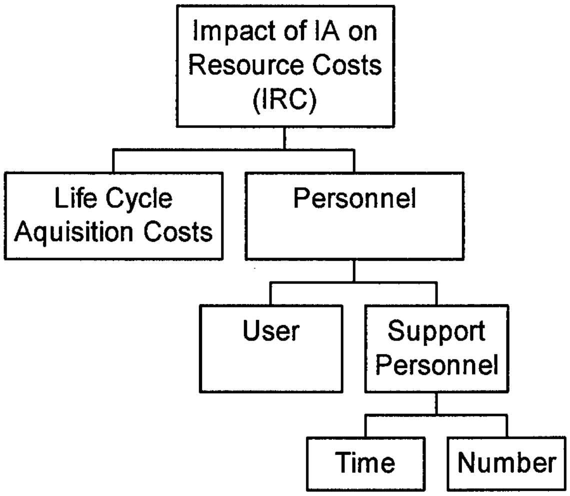
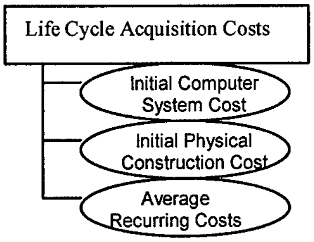

Impact of IA on Resource Costs (IRC)
Life Cycle Aquisition Costs
Personnel
User
Support Personnel
Time
Number

Figure A-57: Impact of Information Assurance on Resource Costs

Impact of IA on Resource Costs: The impact an IA strategy will have on both workforce and fiscal costs.

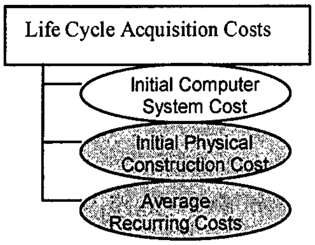
Rationale: All other things being equal, the system that consumes the least amount of AFTAC resources will be the more desired system.


Life Cycle Acquisition Costs
Initial Computer System Cost
Initial Physical Construction Cost
Average Recurring Costs

Life Cycle Acquisition Costs: The fiscal cost of an IA strategy.

Rationale: Budget constraints and monetary resources force cost to be a consideration when determining an IA strategy.

Measure: There are two separate costs to consider when dealing with an IA strategy: the initial cost to purchase the product, and the maintenance costs it will consume over a period of time. Initial costs were separated into computer systems and physical systems since they are treated differently by Air Force regulations.


Life Cycle Acquisition Costs
Initial Computer System Cost
Initial Physical Construction Cost
Average Recurring Costs

<u>**Initial Computer System Cost:**</u> Air Force regulations require that any computer system purchase over $100,000 must be approved by the Air Force. Therefore, any purchase under $100,000 receives a very high value since it can be executed within AFTAC. In addition, purchases under $100,000 can be done more rapidly than larger purchases due to the approval process. Once the $100,000 threshold is crossed, there is a severe drop in value. Any computer system strategy that requires an initial investment of over $1 million scores as no value on this measure.

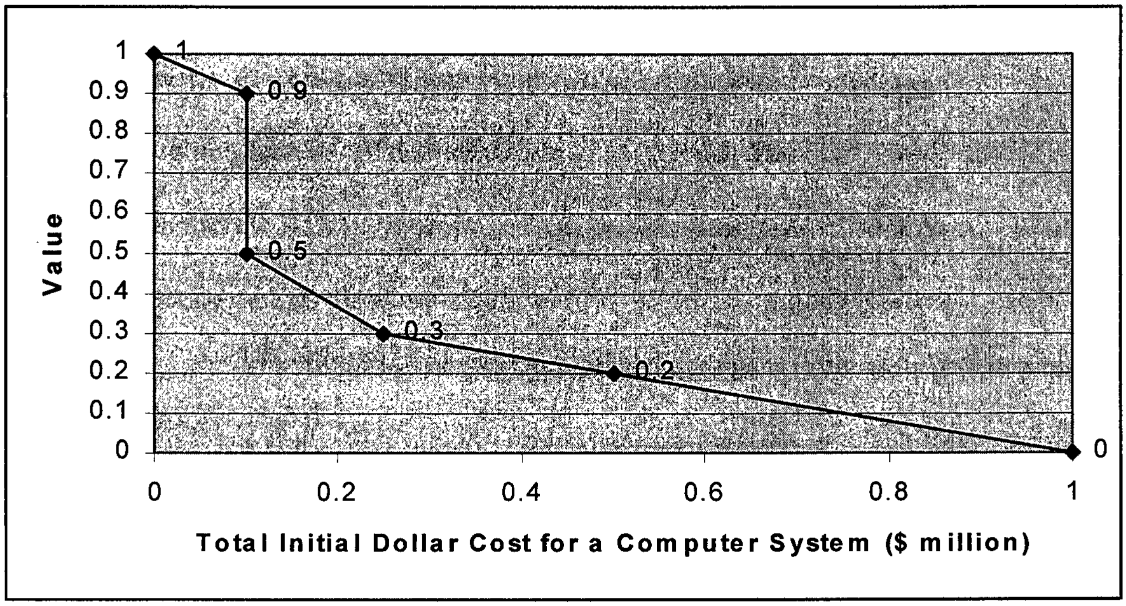
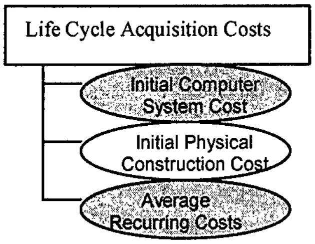


Figure A-58: Initial Life Cycle Acquisition Cost for a Computer System, measured in millions of dollars


Life Cycle Acquisition Costs
Initial Computer System Cost
Initial Physical Construction Cost
Average Recurring Costs

Initial Physical Construction Cost: The curve for initial dollar cost for physical construction is shaped the same as it is for computer systems, although the dollar breakpoints are different. Air Force regulations state that any physical construction under $500,000 does not need to be authorized outside the agency; however once that point is crossed Air Force authorization is required. Such authorization requires more time to attain and is thus less valuable to AFTAC. Therefore, if a physical IA strategy can be accomplished for under $500,000, it will receive high value score (over 0.9). Any physical construction over $5 million will receive no value.

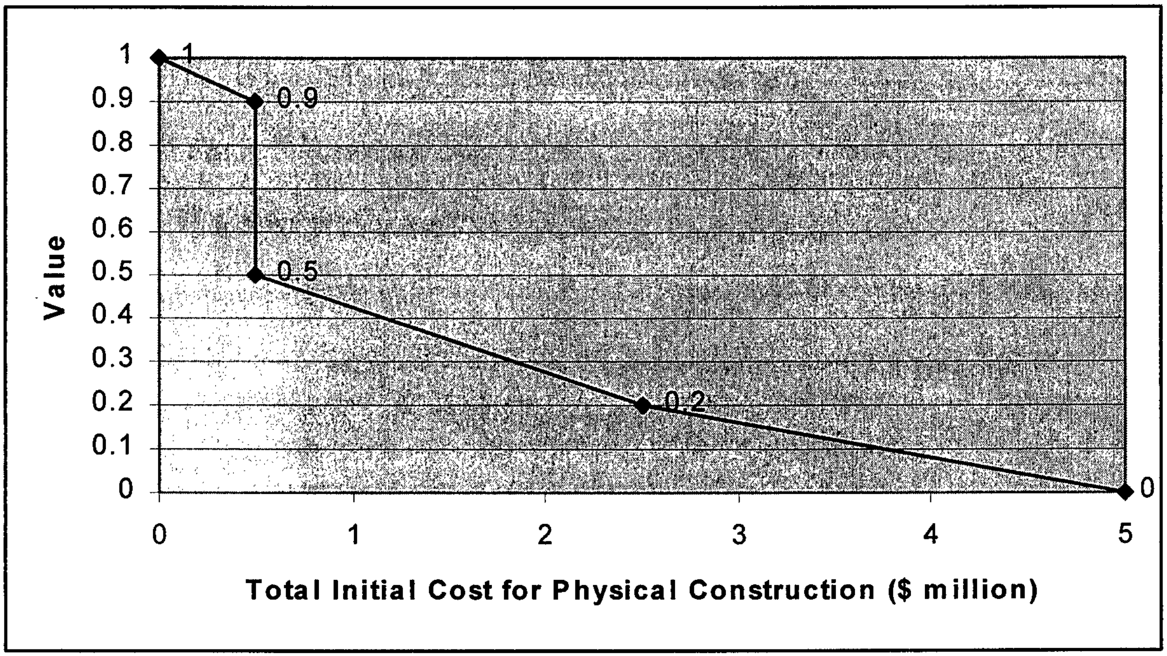
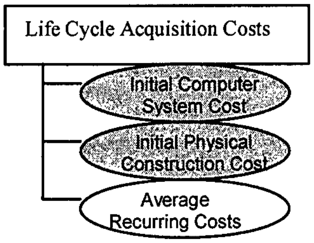


Figure A-59: Initial Life Cycle Acquisition Cost for Physical Construction, measured in millions of dollars


Life Cycle Acquisition Costs
Initial Computer System Cost
Initial Physical Construction Cost
Average Recurring Costs

Average Recurring Costs: Regardless of the type of strategy, recurring costs are considered equally. This graph shows that every dollar is considered to be as valuable as the next, resulting in a linear relationship from $0 to $200,000. Every dollar that can be saved is valuable to AFTAC. After $200,000/yr, no value is earned on this measure.

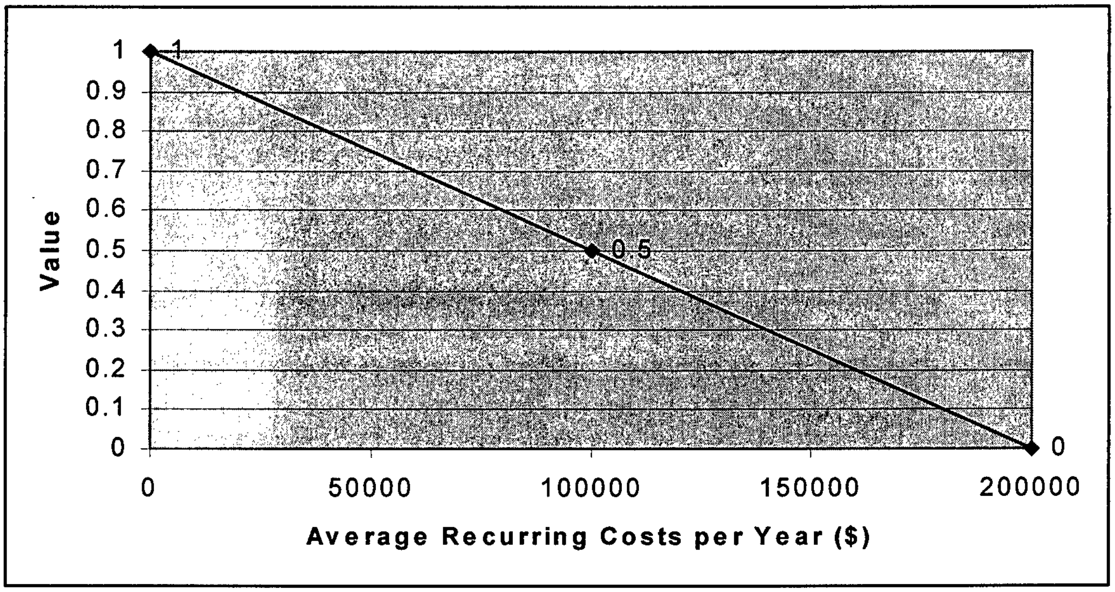


Figure A-60: Recurring Cost of an IA strategy, measured as the Normalized Unit Annual Cost per Year

Personnel

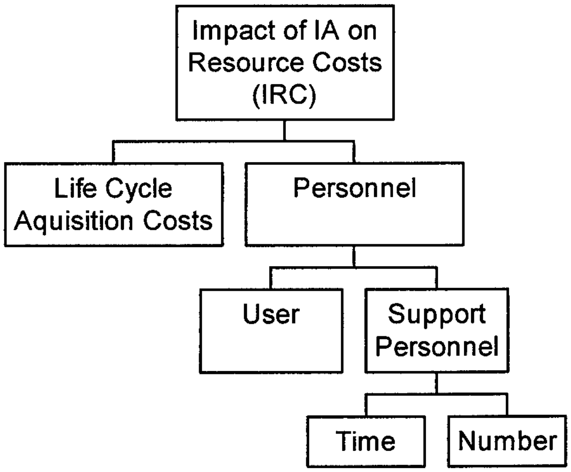
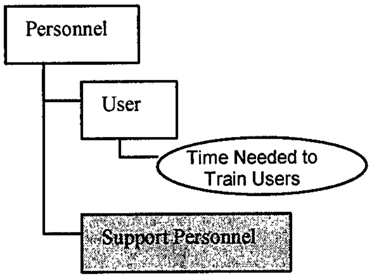

Impact of IA on Resource Costs (IRC)
Life Cycle Aquisition Costs
Personnel
User
Support Personnel
Time
Number

Figure A-61: Personnel

Personnel: The workforce cost of an IA strategy.

Rationale: Implementing an IA strategy may impact the ability of people to perform the mission. Since users and support personnel have separate costs associated with them (user time learning IA is considered different then support personnel time because it takes away the user from the actual mission), they are treated separately in the hierarchy.

User: The amount of user time needed to learn an IA strategy



Rationale: The more time a user spends training as a result of a new IA strategy, the less time they will have to perform their primary mission

Measure: User training time is measured in hours because user time is highly valued. Taking people away from their primary job in order to train them in IA means that they are not performing their mission during this time. Ideally, all user training should be accomplished within a half-hour. After an hour there is a severe value drop. After four hours, no value is scored.

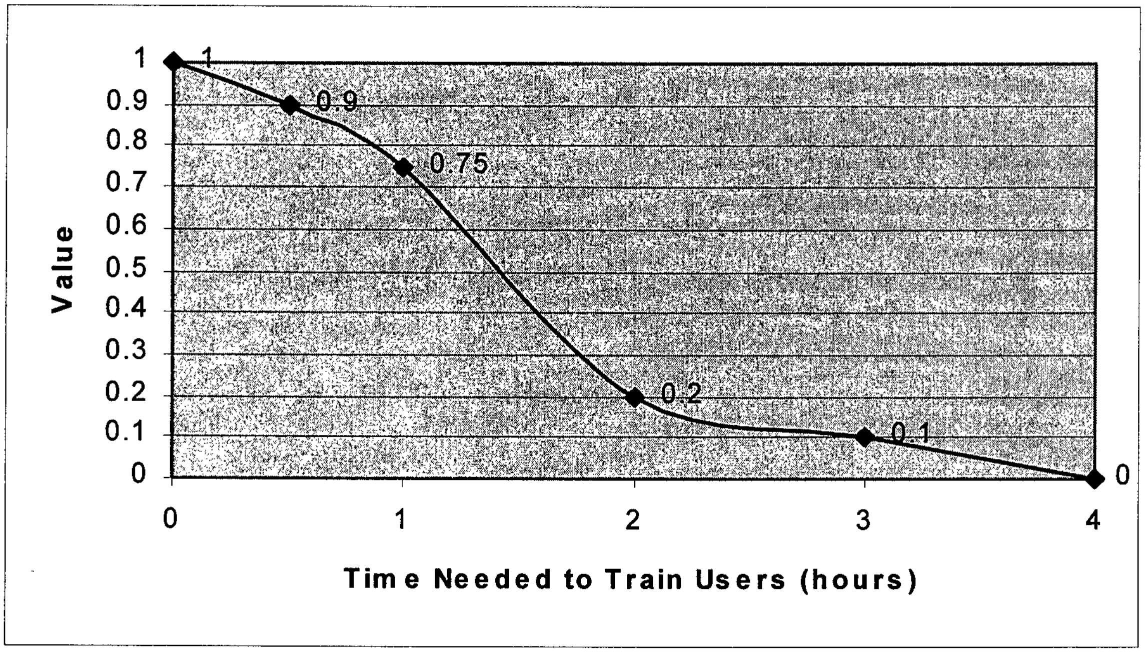
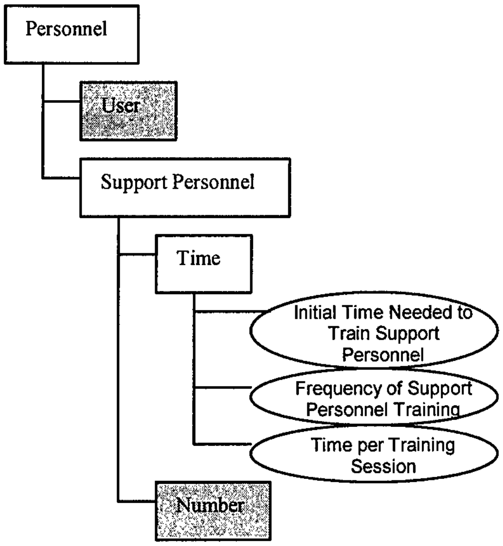


Figure A-62: Time Needed to Train Users, measured in hours


Personnel
User
Support Personnel
Time
Initial Time Needed to Train Support Personnel
Frequency of Support Personnel Training
Time per Training Session
Number

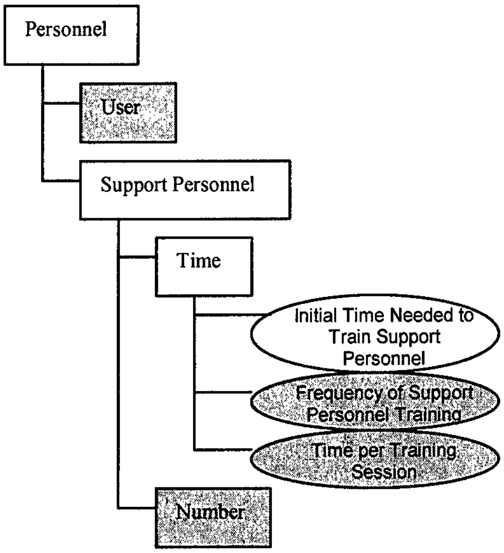
Support Personnel: The amount of added training and people needed to support an IA strategy, broken down further into time and number.

Time: The amount of time needed to train support personnel in an IA strategy.

Rationale: Support personnel will not be able to perform their mission while they are actively training in an IA strategy.

Measure: The Time Needed to Train Support Personnel is composed of the initial training period and recurring training over the course of the year.

Initial Time Needed to Train Support Personnel: Initial training is considered to be the initial exposure of that person to the new strategy. Since the support personnel need to be experts in the strategy, several workdays training is not uncommon. There is a steep drop in value after four workdays, however, because this is the point at which the training has severely taken the administrator away from their primary mission. Lengthy Temporary Duty (TDY) assignments are therefore not desirable. There is another drop after five workdays. After twenty workdays, or about one months' time in training, there is no value to be gained. Every time support personnel must attend training, they force the rest of the organization to function without them. When they are gone for long blocks of time, this can cause a heavy burden on the remaining personnel and users.


Personnel
User
Support Personnel
Time
Initial Time Needed to Train Support Personnel
Frequency of Support Personnel Training
Time per Training Session
Number

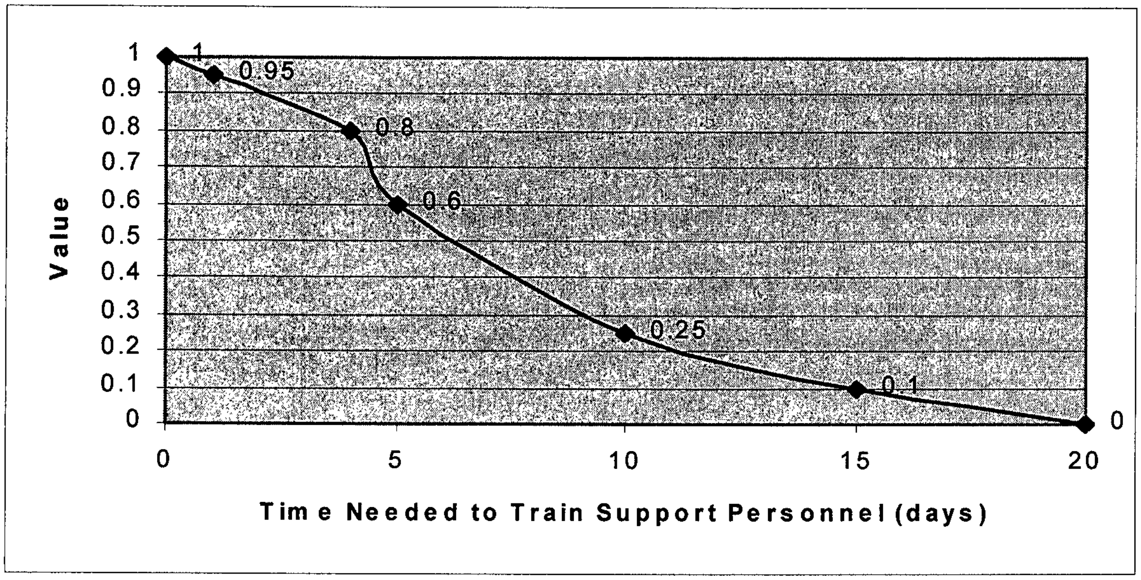
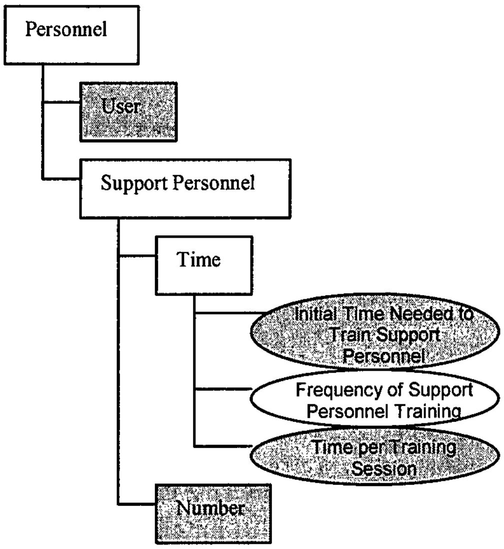


Figure A-63: Time Needed to Initially Train Support Personnel in an IA strategy, measured in workdays


Personnel
User
Support Personnel
Time
Initial Time Needed to Train Support Personnel
Frequency of Support Personnel Training
Time per Training Session
Number

Recurring: The degree of training that support personnel must attend per IA strategy over the course of the year. It is composed of both how often the training occurs (frequency), and how long the training lasts per session.

Frequency: How often the training occurs over the course of the year.

Measure: This value is measured by how often support personnel are taken away from regular duties to train in an IA strategy. Both Daily and Weekly score a 0.0 since this is considered to be too much of a burden on the person and the unit. A strategy that requires recurring training once per year or less often will receive the maximum value of 1.0.

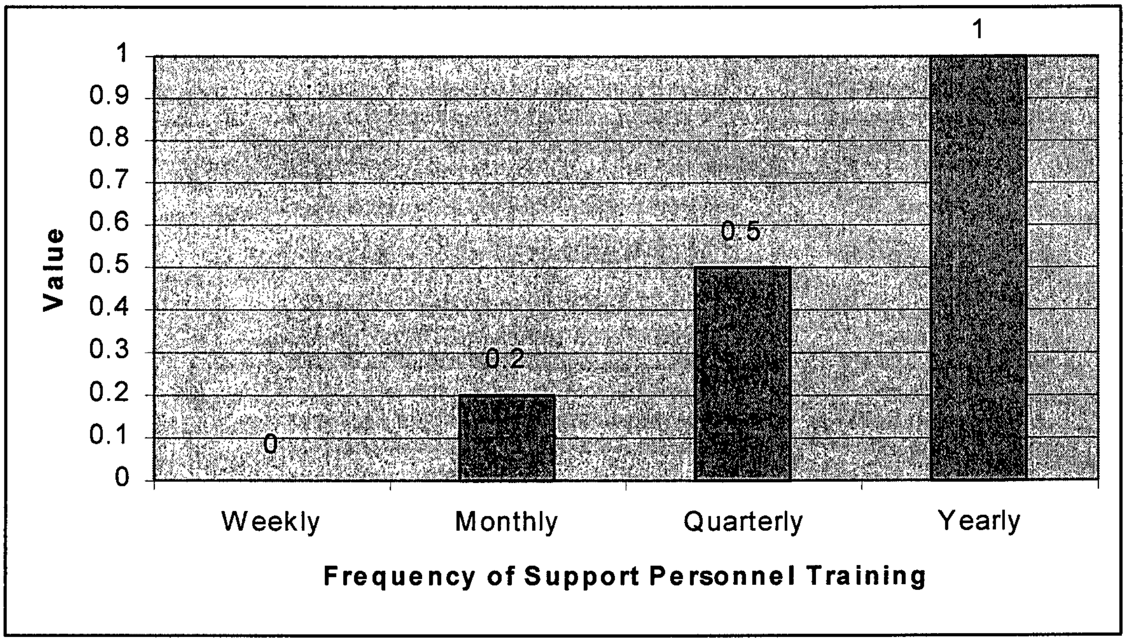
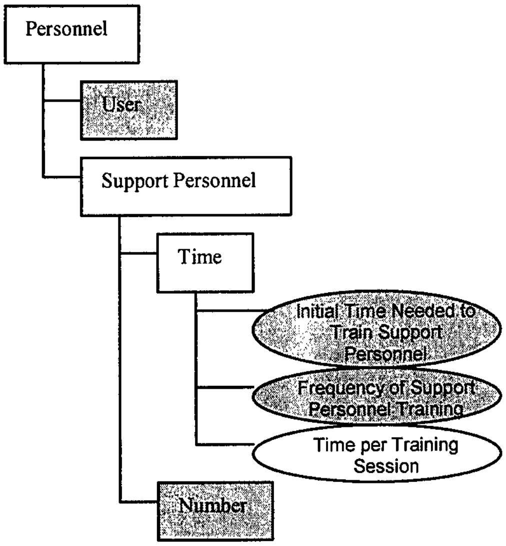


Figure A-64: Frequency of Training Needed for Support Personnel


Personnel
User
Support Personnel
Time
Initial Time Needed to Train Support Personnel
Frequency of Support Personnel Training
Time per Training Session
Number

Time per Training Session: Independent of the frequency of training is the time per training session. Each day is considered valuable, supporting a steep drop off after every full day. Recurring training that lasts over three workdays receives a score of 0.0. Recall that this is measuring recurring training in strategies that personnel are already considered to be experts.

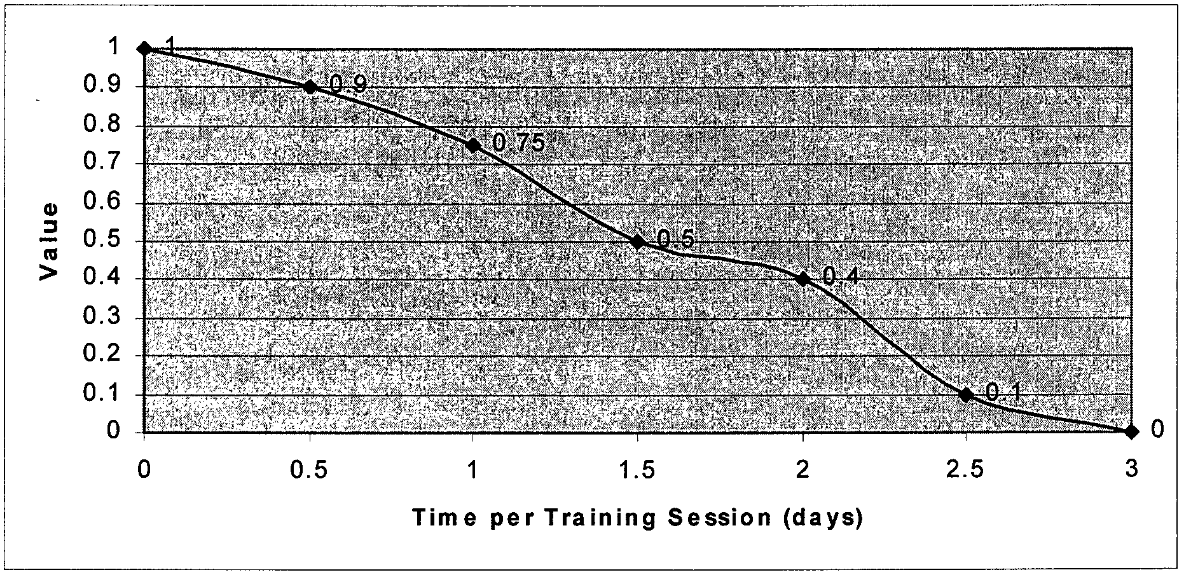
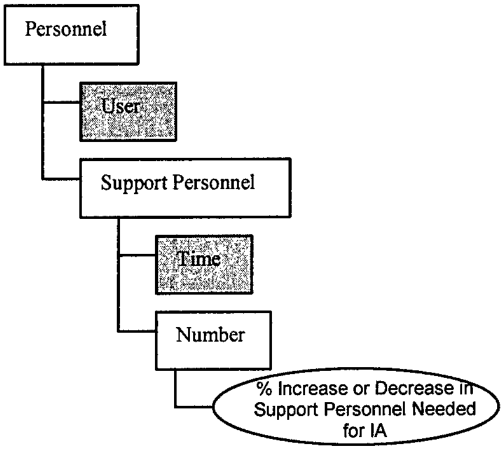


Figure A-65: Time Needed per Training Period for Support Personnel, measured in workdays



Number: The change, either positive or negative, in the number of people needed to perform an IA strategy.

Rationale: All things being equal, an IA strategy that requires one support person will be a better strategy than one that requires two. It is unlikely that an organization will be able to request personnel be moved (either into or out of the organization) depending on their current IA situation; however, it is possible that some support personnel will have the ability to perform other duties should an IA strategy free up some of their time.

Measure: This value is measured as the Percent Change in the Number of Support Personnel required after a new IA strategy. This graph is very sensitive to change, since a loss or gain of 10% is a considerable amount of people. The graph exhibits a steeper value change for adding personnel than for freeing up personnel. As previously mentioned, this is due to the belief that it would be difficult to add personnel.

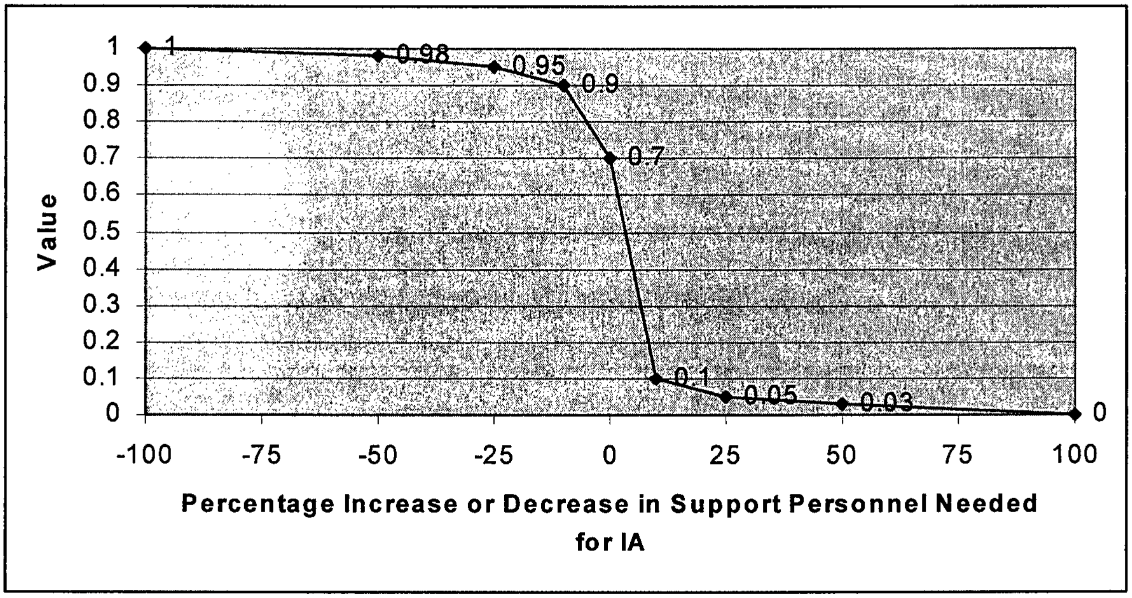


Figure A-66: Percent Change in Support Personnel Needed due to implementing a new IA strategy

BIBLIOGRAPHY

Air Force Computer Emergency Response Team (AFCERT). Kelley AFB TX, 2001. Excerpt from published report, http://afcert.csap.af.mil/.

Air Force Technical Applications Center (AFTAC). Patrick AFB FL. Unpublished report on INFOCON Levels, 2001.

AFTAC / Logistics Support Center (LSC). Patrick AFB FL. Personnel interviews. 13-15 December 2000, 4-5 January 2001, 18-19 January 2001.

CERT / Coordination Center (CERT / CC). *About the CERT/CC.* Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 27 November 2000. Excerpt from published report, http://www.cert.org/nav/aboutcert.html.

CERT / CC. *CERT® Advisory CA-2000-04 Love Letter Worm..* Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 9 May 2000. Excerpt from published report, http://www.cert.org/advisories/CA-2000-04.html.

CERT / CC. *CERT / CC Statistics: 1988 – 2000.* Pittsburgh: Carnegie Mellon Software Engineering Institute, 15 February 2001. Excerpt from published report, http://www.cert.org/stats/cert_stats.html.

Chairman of the Joint Chiefs of Staff (CJCS). CJCS Memorandum CM-510-00, 1999. Washington: Pentagon, 1999.

Cisco Systems, Inc. *Cisco Secure Intrusion Detection.* Excerpt from published report, http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/

Department of the Air Force. *Air Force Basic Doctrine*. AFDD 1. Washington: HQ USAF, September 1997.

Department of the Air Force. *Information Operations.* AFDD 2-5. Washington: HQ USAF, 5 August 1998.

Department of Defense, Joint Chiefs of Staff. *Information Assurance: Legal, Regulatory, Policy and Organizational Legal, Regulatory, Policy and Organizational Considerations*. (Fourth Edition). Washington: Pentagon, August 1999.

Department of Defense, Joint Chiefs of Staff. *Joint Publication 3-13, Joint doctrine for Information Operations*. Washington: Pentagon, 9 October 1998.

Donohue, James P. "Litigation in Cyberspace: Jurisdiction and Choice of Law a United States Perspective." American Bar Association Committee on Law of Commerce in Cyberspace. Seattle: Miller, Nash, Wiegner, Hager & Carlson LLP, 1997.

Doyle, M. P., Deckro, R. F., Jackson, J. A., and J. M. Kloeber. *A Value Function Approach to Information Operations MOE's: A Preliminary Study.* Air Force Institute of Technology Center for Modeling Simulation and Analysis: CMSATR 97-04, July 1997.

Gromov, Gregory R. "History of Internet and WWW: The Roads and Crossroads of Internet History." Excerpt from published report, http://www.internetvalley.com/intval.html.

Hamill, Jonathan Todd. *Modeling Information Assurance: A Value Focused Thinking Approach.* MS thesis, AFIT/GOR/ENS/00M-15. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2000.

Harrow, Jeffrey R. *Not so Secret Agents.* Online periodical: The Rapidly Changing Face of Computing, 2 November 1998. Available at http://www5.compaq.com/rcfoc/981102.html#Not_So_Secret.

Holzinger, Al. "Information Security Management and Assurance: A Call to Action for Corporate Governance." Information Systems Security: 32-40 (May – June 2000).

Internet Security Systems (ISS), Inc. *Internet Scanner Product Specification Sheet.* 2001. Excerpt from published report, http://www.iss.net/customer_care/resource_center/product_lit/.

Keeney, R. L., "Using Values in Operations Research." *Operations Research*: 793-813 (September-October 1994).

Kirkwood, C. W., *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets*. Belmont: Duxbury Press, 1997.

Longstaff, T. A., Ellis, J. T., Hernan, S. V., Lipson, H. F., McMillan, R. D., Pesante, L. H., and D. Simmel. *Security of the Internet.* Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 1997. n. pag. Excerpt from published article, http://www.cert.org/encyc_article/tocencyc.html.

National Information Assurance Partnership (NIAP). *About NIAP.* Gaithersburg MD: 31 January 2001. Excerpt from published report, http://niap.nist.gov/.

NIAP. *Common Criteria Evaluation and Validation Scheme: Introduction.* Gaithersburg MD: 7 April 1999. Excerpt from published report, http://niap.nist.gov/cB-scheme/SchemeIntroduction.html.

President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Thinking Differently*. Washington: GPO, October 1997. Available at http://www.infowar.com.

Symantec, Inc. *Enterprise Security Manager*. Excerpt from published report, http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=45&PID=2229776.

Valeri, Lorenzo. "Securing Internet Society: Towards an International Regime for Information Assurance." Studies in Conflict & Terrorism: 129-147 (April – June 2000).

Zakon, Robert H. "Hobbes' Internet Timeline v5.2." 19 November 2000. Excerpt from published article, http://info.isoc.org/guest/zakon/Internet/History/HIT.html.

VITA

Joseph Edward Beauregard was born in Danvers, Massachusetts on 24 April 1977 to his parents. After graduating from Manchester High School West in 1995, he accepted an appointment to attend the United States Air Force Academy in Colorado Springs, Colorado. Joseph graduated from the Academy in June, 1999 and accepted his commission as a 2nd Lieutenant in the United States Air Force. His first assignment was to Wright-Patterson AFB, Ohio to attend graduate school in the Air Force Institute of Technology's Graduate of Operations Research Master's degree program. Upon graduation from AFIT, 2nd Lieutenant Beauregard will be assigned to the 311th Human Systems Wing at Brooks AFB, Texas as a scientific analyst.