The Total Enterprise Assurance Management (TEAM) Model: A Unified Approach to Information Assurance Management

By

Benjamin L. Tomhave

A Thesis Submitted to the Faculty of
The School of Engineering and Applied Science
in Partial Fulfillment of the Requirements for the degree of
Master of Science

COMMITTEE:

Research Director: Julie J.C.H. Ryan, D.Sc.

Dr. Lance J. Hoffman
Dr. E. Lile Murphree, Jr.

The George Washington University
Washington, D.C.
Spring 2006

Table of Contents

Table of Figures

Abstract

This research thesis addresses the problem of identifying or creating a unified information assurance management model that harmonizes the key competency areas of enterprise risk management, operational security management, and audit management. The research was conducted by performing a literature review of existing information assurance related models, frameworks, and methodologies; creating a new model to unify the three competencies (given the absence of such a model); and, validating the research results with subject-matter experts (SMEs). The research concluded with the development of the Total Enterprise Assurance Management (TEAM) model that was positively validated by the SMEs. Survey results demonstrated that the work was viewed as favorable and logical with a majority of respondents confirming that all four hypotheses of the research had been achieved.

Acknowledgements

The following people are to be recognized for their contributions as subject-matter experts who validated the work in accordance with Phase 3, described herein. These individuals provided direct feedback and/or participated in a standardized survey designed to validate findings:

- John McCumber, Professorial Lecturer, The George Washington University
- Bob Small, CISSP, Principal Member, Technical Staff, Systems and Software Consortium, Inc.
- Timothy Phillips CD, CISSP, Business Group Leader / Executive Consultant, Information Assurance Solutions
- Robert M. Slade, CISSP
- Donn B. Parker, CISSP, Retired Information Security Consultant
- Dr. Ralph May, Adjunct Lecturer, Whiting School of Engineering, Johns Hopkins University
- Rick Murphy, Sr. Principal Infosec Scientist, Mitretek Systems
- William (Bill) Boni, Vice President - Information Security and Protection, Motorola
- Dr. Fred Gallegos, CISA, CDE, CGFM, CIS Dept., College of Business, California State Polytechnic University, Pomona
- Mark Kadrich, CISSP, Senior Principle, Symantec
- Kenneth R. van Wyk, Principal Consultant, KRvW Associates, LLC
- Esther Czekalski, CISSP

Additionally, the following people are to be thanked for their support of the author throughout the process of creation, development and documentation, whether it was in providing work flexibility, being a sounding board for ideas, or simply through supporting the effort:

- Hanna Tomhave (wife)
- Dr. Julie Ryan (GWU, advisor)
- Robert Alberti, Jr. (friend, editor)
- Paul Nguyen (friend)
- T. Ben Mayrides (AOL, direct manager)
- David Merkle (formerly AOL, group director)
- Levena Bailey (AOL, department VP)
- Joseph Abramson (AOL, statistician)
- Dr. William K. Tomhave (Concordia College, editing)

Abbreviations

COBIT	Control Objectives for Information and related Technologies
ERM	Enterprise Risk Management
FISMA	Federal Information Security Management Act, part of the Electronic Government Act of 2002
GLBA	Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999
HIPAA	Health Insurance Portability and Accountability Act of 1996
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITGI	Information Technology Governance Institute
InfoSec	Information Security
PCI DSS	Payment Card Industry Data Security Standard, also known from Visa as the Cardholder Information Security Program (CISP)
SOX	Sarbanes-Oxley Act of 2002

Glossary

Approach. A generic term for a structured description of how to do something, ranging from a high level (such as with a model), a moderately detailed level (such as with a framework), or a targeted and detailed level (such as with a methodology).

Baseline. A low-level, specific set of requirements and recommendations that provide detailed operational directions for conformance and compliance with policies and standards.

Framework. A fundamental construct that defines assumptions, concepts, values, and practices, and that includes guidance for implementing itself.

Guideline. A mid-to-low-level set of guidance designed to help operations align with business requirements and strategy.

Method. A term used synonymously with approach (defined above).

Methodology. A targeted construct that defines specific practices, procedures and rules for implementation or execution of a specific task or function.

Model. An abstract, conceptual construct that represents processes, variables, and relationships without providing specific guidance on or practices for implementation.

Policy. A high-level statement of requirements, often in business language, that sets and/or communicates strategic direction.

Procedure. Documentation of specific steps required to complete a task, aligned with policies, standards, and baselines.

Standard. A mid-level set of requirements that translate policy statements into actionable statements, bridging the gap between business and operations.

I. Introduction

The concept of "security" has existed for ages, manifesting itself most commonly in the protection of material things, people, and secrets. With the advent of the digital age, a field has emerged that is invoked variously by the name "computer security," "data security," "information security," or even "information assurance." Additionally, related fields have also emerged, such as "enterprise risk management" and "audit management." The various names belie the commonality of the endeavors, each of which is focused at protecting and defending information assets and systems. Simultaneously, these variously-named fields have arisen during a period of time in which we see the devolution of organizing principles that have guided enterprise endeavors to protect information assets. The result has been a proliferation of approaches that serve more to confuse than to guide enterprise efforts to protect information assets and systems.

The purpose of this research is to determine if that situation can be rectified through the development of a unified model (by "unified" here we're talking about a single approach that brings key competencies together, not unification in the sense of merging competencies into a single mega-competency). The research first identified and classified the numerous and varied information assurance methods used throughout industry and government. Upon completion, a combined single method that can supersede all others was developed. This single method represents a unified model that can be used by many different enterprises. The resulting unified model – the Total Enterprise Assurance Management (TEAM) model – has been validated through directly elicited judgment by subject matter experts with their feedback incorporated into the model.

Statement of the Problem

Despite the numerous models, frameworks, and methodologies used throughout industry and government to address enterprise risk management, operational security management, and audit management, there is no overarching model that brings these offsetting areas of need into a single, harmonized organizational structure. This research seeks to create such a unified model, harmonizing the key competency areas of enterprise risk management, operational security management, and audit management under a single information assurance management model. Successful solution of the stated problem should result in a more effective and efficient approach to managing the complex challenges associated with security.

Organization of the Document

This document is organized into five sections. The first section provides an introduction to the research, including background, purpose, significance, scope, and limitations. Section two, Literature Review, provides a high-level survey of research material covered. This section was originally supplemented by a standalone white paper. The content of the white paper has since been fully integrated into the body of this document. The research goals and hypotheses are stated in section three. Section four comprises the core analysis of the research and presents the model developed to accomplish the stated objectives. Last, section five recapitulates research findings, summarizes feedback from subject matter experts through descriptive and inferential analysis, and describes areas for future research.

Background

Existing methods are oftentimes owned by organizations or individuals with a specific focus or mission, potentially resulting in the application of unintended bias. These organizations, in particular, may have professional certifications and memberships that further amplify the unintended bias inherent in the program related to the program focus. This bias may be applied inadvertently as these certified individuals work within organizations when choosing and implementing an information assurance management approach.

The problem created by this potential bias is that organizations may be pushed and pulled in contrary, incompatible directions by individuals who believe in their method and who may not realize their inherent bias. These contradictions in management approaches could result in increased overhead costs for organizations. For example, if two groups are working in parallel to implement different methods, and the methods are diametrically opposed on a given issue, then the groups may reach a deadlock position, or actively work against each other, to the detriment of the organization as a whole.

Given these apparent challenges inherent in relying on sources that may be biased by direct investment in a given approach, it may be preferable for an independent review and classification of methods. Furthermore, the development of an overarching method that could harmonize competing approaches, providing a means for resolving contradictions, may be of value to organizations. This is the intent inherent in this research.

Purpose

The purpose of this research is to develop and validate a unified model that will position both industry and government strongly to counter the competing approaches of external forces, while allowing organizations to build their own approach around their business, first and foremost, and around best practices secondarily within each key area.

Significance

The significance of this research is to establish a formal, universal model that harmonizes the key areas of enterprise risk management, operational security management, and audit management that will allow an organization to first formulate a central, coherent plan, and to then leverage existing best practices in implementing that plan. This approach represents a win-win-win scenario in that organizations will benefit from a single coordinated approach, external forces will benefit from being able to continue using their best practice approaches within each key area, and best practices can continue to evolve in a decentralized, but focused, manner.

Scope and Limitations

Scope

The scope of this research includes the following:

- Identify and classify as many applicable models, frameworks, and methodologies as possible.
- Identify case studies supporting the identified methods.

- Create a unified model that incorporates enterprise risk management, operational security management, and audit management.
- Identify a sample of sources of industry and government regulations, both domestically and internationally, that influence information assurance management practices.
- Validate the findings and proposed management model through informed interviews with industry experts.

Limitations

The research is based on available documentation, case studies, and direct observation. Informal surveys and queries of industry professionals were used to assist in identifying sources and examples. The research does not judge the merits of each identified method, but instead classifies it objectively, relying on the stated purpose contained within the method itself.

Furthermore, it was necessarily acknowledged a priori that there may be significant institutional resistance to this research. As such, it was possible that the research may suffer from lack of participation of the most knowledgeable and capable individuals in the field. Though participation rates in the subject matter expect survey was lower than desired, it is not believed that this lack of participation was due to institutional resistance.

II. Literature Research

Summary

Literature research was performed in three key areas: 1) models, frameworks, and methodologies; 2) case studies supporting these methods; and, 3) regulations applicable to information assurance. This effort reached an initial culmination in a standalone white paper, *Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies v1.0*, in which nineteen (19) methods were identified, classified, and described based upon available documentation. This section contains the content of this white paper in its entirety, with minor editorial corrections. Evolution of this white paper has continued past the scope of this thesis research.

Case studies have been identified from the IT Governance Institute (ITGI), part of the Information Systems Audit and Control Association (ISACA), which specifically address the use of the COBIT framework within organizations. Future research efforts involved with the release of version 2.0 and beyond of the white paper are planned to identify additional case studies outside the scope of COBIT.

Literature covering the topic of applicable regulations includes a review of common legislative and industry specifications, such as the Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Payment Card Industry Data Security Standard (supported by Visa, MasterCard, and American Express). Additional research into the areas of privacy and data protection regulations, as well as an expansion of the initial research, is planned for future releases of the *Alphabet Soup* white paper.

Furthermore, future research may also expand into U.S. Government regulatory structures, such as described within the Clinger-Cohen Act and the Federal Information Security Management Act (FISMA).

It should be noted that the TEAM model exists independent of the resultant white paper from the Literature Review. The purpose of the TEAM model is to provide a high-level model that shapes the assurance function of an organization, while allowing the organization to choose or create the specific approach within each competency area that best matches the needs of the business. As such, while frameworks and methodologies change, mature, deprecate, and so on, the TEAM model is able to stand up resiliently and robustly.

INTRODUCTION

The year is 1995. The Internet is just beginning to blossom, applications like "Mosaic" and "Netscape" begin to bring graphical content to Internet users. Discussions begin to occur frequently about how to use this technology to make money. Five years later, an inflated economy built on such innovation bursts, leaving many "eCommerce" companies bankrupt and slowing growth. In the wake of the economic slide, organizations like the Securities and Exchange Commission (SEC) reveal accounting inconsistencies in major corporations like Enron and WorldCom. At the same time, the United States shudders from the impact of the 9/11 terrorist attacks and soon thereafter launches retaliatory strikes. In the legislative wake of these incidents new laws such as USA-PATRIOT and Sarbanes-Oxley arise. Meanwhile, States, beginning with California, start discussing consumer privacy concerns and passing legislation like California's SB-1386 that mandate that companies notify customers of material breaches of privacy.

Just ten years after the dawn of the Digital Age, we are faced with exponential increases in the regulatory environment, taking the form of GLBA, HIPAA, SOX, and SB-1386 (and other States' similar legislation). Likewise, industry giants like Visa and MasterCard have developed their own data security standards and have begun testing programs to ensure that organizations wishing to conduct credit card business of these types have at least achieved a nominal level of security assurance within their environments. All of this has taken place in the face of greater threat of fraud and identity theft, made worse by the anonymous, mass-proliferating nature of the Internet.

To meet these growing demands, a virtual cottage industry has sprung up across the Internet in the form of information security models, frameworks, and methodologies. Each one of these methods has pros and cons, and oftentimes represents the cumulative effort of large associations of professionals, ranging from business to audit to engineering, and beyond. Unfortunately, for all the methods out there, and for all the regulations (both legislative and industry), there is one thing lacking: clarity. What does it all mean? Should your organization be leveraging any or all of these models, frameworks, or methodologies? Furthermore, what *is* a model, a framework, and a methodology?

Overview of Approach

This literature review attempts to define a taxonomy for these various methods, and then to containerize as many methods as could be identified in a reasonable amount of time within this taxonomy. The list of methods contained within this document was developed with assistance from members of the CISSPforum mailing list, managed by the International Information Systems Security Certification Consortium ($(ISC)^2$). This Literature Review

contains a standardized listing of these methods with an analysis and summary of each method's provisions. This section will also discuss, from a US-centric standpoint, high-profile regulations (legislative and industry) and how the methods described herein can be leveraged against these regulations. Finally, the Literature Review will conclude with closing thoughts.

Author Bias

Before launching into a description and analysis of various information security methods, it is first valuable to state any biases that may affect the objectivity of the author. This author has been working within the Information Technology (IT) arena for over ten (10) years, primarily with an interest in and slant towards information security. In 1994, the author was experimenting with UNIX testing and hardening tools like COPS, TIGER, and crack. Later on, the author began to merge concepts from Management Information Systems courses with a technical background of experience and Computer Science. Today, the author strongly favors an IT alignment approach to information security that seeks to integrate, rather than segregate, IT professionals and infrastructure within an organization. Attempts at demonstrating true return on (security) investment (ROI or ROSI) are believed by this author to be foolish as the true value of most security safeguards is in preventing bad things from happening – something that is impossible to measure (i.e., you cannot prove that something does not exist, only that something does exist). The author strongly prefers a holistic approach versus piecemeal solutions, and has a particular fondness for information security management.

TAXONOMY

In order to properly understand the value and purpose of each method, it is first necessary to define a common language with which to describe them. This task is neither simple nor straightforward given the frequency of word and acronym duplication and misuse. In pondering an effective approach to classifying each method, it was first necessary to consider those words most commonly used within the methods themselves for self-description.

The INFOSEC Assurance Training and Rating Program (IATRP) from the National Security Agency (NSA) has developed a set of INFOSEC Assurance methods that use the following common definition of the "Vulnerability Discovery Triad." (a.k.a., "Vulnerability Analysis Triad") [*35, 36, 37*]

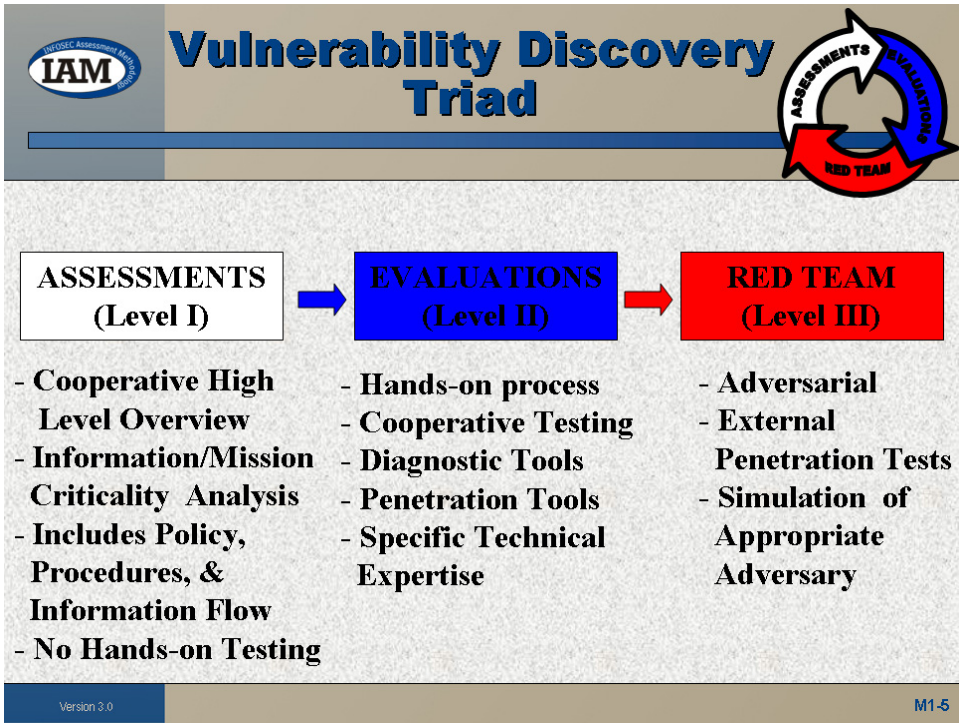

Figure 1: Vulnerability Discovery Triad [*36*]

The problem with the above definition is that it is not consistent with the terminology generally used throughout the security, audit, and governance industries. For example, in most circles an "assessment" is considered a relatively technical, in-depth test of a system, while an "evaluation" is equated to an "audit" or "compliance" type test that is, in fact, less technical. Thus, while it is very useful and helpful for the IATRP to define these three levels of effort, their very inconsistency with the rest of the industry makes their position potentially untenable and incompatible.

As the next step in identifying good taxonomic terms for use in the classification of methods we turn to definitions of the terms by Wikipedia and Dictionary.com. To start, let us define what taxonomy is, if only to ensure that this effort is not misdirected. According to Wikipedia, taxonomy "may refer to either the classification of things, or the principles underlying the classification." [*40*] Dictionary.com further reinforces this notion in their second definition, stating that taxonomy is "The science, laws, or principles of classification; systematics." [*41*]

Having established that taxonomy is the right course, it is then useful to explore the three common terms found in many of these methods: model, framework, and methodology.

Models

The most fitting definition of a model from Wikipedia seems to be for an "abstract" or "conceptual" model, which is defined as "a theoretical construct that represents physical, biological or social processes, with a set of variables and a set of logical and quantitative relationships between them." [*42*] For the purposes of this taxonomy, a model is a high-level

construct representing processes, variables, and relationships. Models are conceptual and abstract in nature and generally do not go into specific detail on how to be implemented. Furthermore, a good model will be independent of technology, providing a generic reference frame.

DEFINITION
A model is an abstract, conceptual construct that represents processes, variables, and relationships without providing specific guidance on or practices for implementation.

Frameworks

Having defined a model as a generic, high-level construct, it becomes clear that another term must be defined to address that class of method that goes beyond the conceptual space and begins to dabble in implementation guidance. The term "framework" seems to fit that bill. Wikipedia lacks a general definition for framework, but says, "In software development, a framework is a defined support structure in which another software project can be organized and developed." [*43*] This definition sounds promising as it hints that a framework provides more detail and structure than a model. Dictionary.com includes two definitions that seem to further reinforce our use of framework in this manner. Definition 3 calls a framework "A fundamental structure, as for a written work." And, definition 4 says that a framework is "A set of assumptions, concepts, values, and practices that constitutes a way of viewing reality." [*44*]

The key differentiator here between a model and framework seems to be in these last definitions. While a model is abstract and conceptual, a framework is linked to demonstrable work. Furthermore, frameworks set assumptions and practices that are designed to directly

impact implementations. In contrast, models provide the general guidance for achieving a goal or outcome, but without getting into the muck and mire of practice and procedures.

DEFINITION
A framework is a fundamental construct that defines assumptions, concepts, values, and practices, and that includes guidance for implementing itself.

Methodologies

Having defined a high-level and mid-level construct, it is then logical to seek a low-level construct that can be used to define those methods that go into specific details for implementation within a focused area. Per Wikipedia, "In software engineering and project management, a methodology is a codified set of recommended practices, sometimes accompanied by training materials, formal educational programs, worksheets, and diagramming tools." [*45*] Definition 1.a. from Dictionary.com reinforces Wikipedia, stating that a methodology is "A body of practices, procedures, and rules used by those who work in a discipline or engage in an inquiry." [*46*]

DEFINITION
A methodology is a targeted construct that defines specific practices, procedures, and rules for implementation or execution of a specific task or function.

DETAILED OVERVIEW AND ANALYSIS

Within this Literature Review are described nineteen (19) different methods falling into one of the three taxonomic areas (model, framework, or methodology). Each method is

described in brief and then afforded a full analysis. Within each taxonomic sub-section, the items are ordered alphabetically so as not to construe preference for one method over another.

A Word on Format

This Literature Review will use a standard format for describing and analyzing each method. While the methods described in this section are pre-sorted into their taxonomic container (model, framework, or methodology), this classification will also be included in the header for each method, so as to facilitate a hasty review. Following is an example of the standard header used throughout this section.

Official Name: (The official full name of the method.)

Abbreviation(s): (Any common abbreviations used for the method.)

Primary URL: (The primary web address of the method.)

Classification: (The taxonomic classification of the method.)

Status: (The current observed status of the method. The following statuses are used within this document:

- *Complete*: The method represents a complete work that can stand on its own.
- *Incomplete*: The method has not been fully developed.
- *Construction*: The method may be complete or complete, but is currently undergoing revisions.
- *Deprecated*: The method is no longer being maintained or revised.)

Stated Objective: (The main stated objective of the method, as described by the method itself. If no official stated objective is listed, then a presumed objective is given and annotated as such.)

Analysis: (A detailed description and analysis of the method. The analysis will provide a thorough description of what the method does, how it can be used, and what pros and cons

may be associated with its use.)

Models

The following method has been determined to be abstract and conceptual in nature, providing general guidance toward achieving an objective without going into specific implementation details. It is classified as a model.

Why is there only one?

It is of great significance here to note that there is, in fact, only one method classified as a model within the context of this document. Whereas several methods were considered as candidates for models – such as IA-CMM, SSE-CMM, ISM3, ISO/IEC 17799:2005, and COBIT – they all failed the definition test for the same reason: they all include extensive practice statements that describe how to implement the method. Only one method did not include practice statements, and as such deserves to standalone. This method meets the definition of a model by being abstract, conceptual, and technology-independent. As such, this model could be applied to other areas outside of information security (such as physical security) with little or no modification of its core tenets.

1. The McCumber Cube

Official Name: "Information Systems Security: A Comprehensive Model"

Abbreviation(s): McCumber Cube, McCumber Model

Primary URL: (none)

Classification: Model

Status: Complete

Stated Objective: To provide an information-centric model that captures the relationship between the disciplines of communications and computer security, without the constraints of organizational or technical changes.

Analysis: As indicated in the Stated Objective above, the McCumber Cube [*31*] is an information-centric model that has been applied to computer security. It focuses on three dimensions of information: Information States, Critical Information Characteristics, and Security Measures. Within each dimension are three aspects, which, when coupled, result in a three-dimensional cube where each dimension is on an axis of the cube.

Unlike the frameworks described below, the McCumber Cube does not go into details on implementation, such as with extensive practice statements. Instead, [*31*] discusses examples of how the model can be used within an organization after first providing a foundational discussion of computer security (or information security, or information assurance, depending on your preferred term today) and introducing the model in its entirety.

This model is very useful for understanding a highly complex topic (computer security) in a very concise, albeit abstract, manner. Furthermore, the focus on information allows the model to be applied to other topics beyond security with relative ease.

The downside to the model is that it does not provide detailed implementation details. Thus, in order to make use of the model, one must first understand it and translate that understanding into an achievable objective or task. As such, selling this concept to senior management may succeed or fail, depending on their ability to grasp the overall picture presented.

As a high-level model, the McCumber Cube is a very valuable tool for assessing an organization to help focus resources. It would be very useful

combined with a compatible framework and methodology from the following sections.

Frameworks

The following eleven (11) methods have been determined to provide general guidance toward achieving an outcome without going into specific detail on a single focused task. Each of these methods has been classified as a framework.

1. Control Objectives for Information and related Technology

Official Name: Control Objectives for Information and related Technology

Abbreviation(s): COBIT, COBIT

Primary URL: http://www.isaca.org/cobit/

Classification: Framework

Status: Complete, Construction

Stated Objective: "The COBIT Framework provides a tool for the business process owner that facilitates the discharge of" business process responsibilities. [*23, p.4*]

Analysis: COBIT [*20-29*] is an IT-centric framework designed to provide users, businesses, and auditors with a standard approach for designing, implementing, and testing IT controls. This framework has been universally developed and adopted by the Big N audit houses as a solution to most IT audit, compliance, and governance "problems."

The framework provides maturity models, critical success factors, key goal indicators, and performance indicators, all for use in managing Information and related Technology. Additionally, COBIT defines control objectives and audit guidelines to support its implementation. These

practice statements go into sufficient detail to instruct an IT or audit practitioner in how to best implement the framework.

At the core of COBIT is a cyclical process that circles around "Information" and "IT Resources." The four phases (or domains, as COBIT calls them) of the cycle are "Planning & Organisation," "Acquisition & Implementation," "Delivery & Support," and "Monitoring." The cycle starts with "Information" that has ties to COBIT and "IT Resources," and then leads to P&O, which leads to A&I, which leads to D&S, which leads to Monitoring. Each of the four domains defines detailed, specific practices for implementation.

COBIT is best summed by this process-flow statement, found in [*24, p.21*]: "The control of IT Processes which satisfy Business Requirements is enabled by Control Statements considering Control Practices."

At its best, COBIT is a very thorough framework for defining, implementing, and auditing IT controls. For audit organizations, either internal or external, that are hoping to get their hands around the oftentimes challenging task of ensuring that effective controls are in place on key systems ("financially significant" in the SOX vocabulary), then COBIT is exactly what the doctor ordered.

Unfortunately, COBIT can be a very confounding framework for information security practitioners. For starters, COBIT is ***not*** an information security framework. It is an IT controls framework, of which infosec represents one (1) practice out of 34. Furthermore, to implement COBIT within an organization means dedicating an extraordinarily significant amount of resources to the task. In this day and age of decreasing operational budgets and increasing threats and regulatory burden, it is not reasonable to expect that an organization can readily implement all of COBIT.

Moreover, there is no obvious security benefit for

an organization to implement COBIT. Information security, being a holistic problem that must be addressed at all levels of an organization, is not IT-specific. As such, any overall framework implemented to improve the information security posture of an organization needs to speak to those different levels, and not be bound painfully to one focus (IT).

If one were to listen to the guidance of public accounting firms, one might think that COBIT was the best solution for solving security problems. What one would need to bear in mind, however, is that COBIT was developed by the Big N audit firms, for the Big N audit firms. Deployment of COBIT across an organization provides the added benefit to the audit firms of being able to reduce total hours spent on an annual audit, thus reducing the investment in personnel required, optimizing the profitability of the engagement. Whether or not the organization being audited will see any cost savings from implementing COBIT is debatable. And, in the end, the organization will not have addressed information security, but instead addressed the auditability of its IT resources.

[*8*] is an excellent reference for implementing COBIT-style controls and performing audit functions in a manner consistent with those prescribed in COBIT and by the ISACA, the AICPA, and the PCAOB.

Note: Please see the note above for concerns on any apparent author bias that may be represented here.

2. Common Criteria

Official Name: Common Criteria for Information Technology Security Evaluation

Abbreviation(s): ISO/IEC 15408, CC

Primary URL: http://www.commoncriteriaportal.org/ or http://niap.nist.gov/cc-scheme/index.html

Classification: Framework

Status: Complete, Construction

Stated Objective: From [*16, Part 1, p.9*]:
"The CC permits comparability between the results of independent security evaluations."

"The CC is useful as a guide for the development, evaluation and/or procurement of (collections of) products with IT security functionality."

"The CC is applicable to IT security functionality implemented in hardware, firmware or software."

Analysis: The Common Criteria [*16*] is a framework for describing the "IT security functionality implemented in hardware, firmware or software." [*16, Part 1, p.9*] It is an ISO/IEC Standard that originated with federal governments in Canada, Europe, and the United States. It represents an evolution beyond previous infosec frameworks, such as the Trusted Computer Security Evaluation Criteria (better known as the Orange Book).

Common Criteria is not a framework that will better secure an organization. In fact, it has nothing to do with implementing security within an organization. Instead, the CC is used as a lingua franca for product vendors to describe the IT security requirements of their products for use in evaluating the level of assurance that can be placed in that product. Vendors target an Evaluated Assurance Level (EAL) based on business requirements (their own, or their customers') and then submit a Protection Profile with the product to be evaluated against the EAL.

CC has been included in this document for completeness and as a means to educate users outside the federal sector on the goals of the CC. It should also be noted that the current draft version of CC, v3.0, was reviewed for this paper.

3. COSO Enterprise Risk Management – Integrated Framework

Official Name: The Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management – Integrated Framework

Abbreviation(s): COSO, COSO ERM

Primary URL: http://www.coso.org/

Classification: Framework

Status: Complete, Construction

Stated Objective: To provide a business-oriented framework for implementing enterprise risk management.

Analysis: COSO [*9, 10*] is a comprehensive framework for the implementation of enterprise risk management through an integrated approach. It uses a matrix type method in referencing four categories of objectives to eight components of enterprise risk management to an entity's four units.

The four categories of objectives defined by COSO are: strategic, operations, reporting, and compliance. The four units of an entity are defined as entity-level, division, business unit, and subsidiary. Finally, the eight components of enterprise risk management are:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

COSO defines enterprise risk management as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed

to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." [*9, p.2*]

The COSO study advocates a top-down approach to implementing and testing the enterprise risk management framework within an entity, putting the responsibility squarely on the shoulders of the top executives. This guidance is consistent with the Sarbanes-Oxley legislation discussed below.

The current iteration of COSO, released in 2004, came about in response to the issuance of SOX in 2002. It is a follow-up study to the original COSO report released in 1987. The framework advocated in the original release has been significantly updated in this model with an eye toward improving corporate responsibility and governance while placing strong emphasis on senior management needing to own responsibility for successes and failures in the area of enterprise risk management.

The COSO framework itself provides practice statements and guidance for implementing the advocated enterprise risk management solution. Access to the official report must be purchased, but a pre-final draft was circulated in 2004 prior to publication. This draft was generally organized according to the components of enterprise risk management.

Whereas COSO and COBIT are oftentimes correlated, reading the draft COSO manuscript represents a stark contrast to COBIT. COSO talks at length about identifying and managing business risks, while COBIT is focused exclusively on IT controls. As such, COSO is more inline with frameworks like ISO/IEC 17799 and the various CMM derivations.

What COSO does not provide is a methodology for actually assessing and mitigating risks. This, however, is not the focus of the study. As such, if an organization were to adopt the COSO approach

to enterprise risk management, it would then be necessary to also develop and implement a methodology for assessment and mitigation of risks. This is common to all frameworks reviewed during this study.

As a final pronunciation, COSO represents a very useful tool for the organization. Not only does it describe an enterprise risk management framework, but it also provides guidance on selecting supporting methodologies that would integrate with this framework. As such, it is by far one of the most comprehensive frameworks reviewed in this paper.

4. Information Security Management Maturity Model

Official Name: Information Security Management Maturity Model

Abbreviation(s): ISM3, ISMMM

Primary URL: http://www.isecom.org/projects/ism3.shtml

Classification: Framework

Status: Complete, Construction

Stated Objective: Offer "a new approach for specifying, implementing, operating and evaluating ISM systems…" [*6, p.5*]

Analysis: ISM3 [*6, 7*] uses a capability maturity model approach in developing a process-oriented framework that is technology-independent for managing information security management systems (ISMs or ISMS). The goals of ISM3 are to prevent and mitigate incidents, as defined using "Security in Context," and to optimize business resources.

ISM3 is comprised of four practices – one generic and three specific. The generic practice is called "Documentation" and the three specific practices are called "Strategic Management," "Tactical

Management," and "Operational Management." The generic practice is applicable to all three specific practices and describes requirements for document management.

Each of the three specific practice areas targets a horizontal within the business. These practices assume that an organization can be divided into functionally separate task groupings: strategic, tactical, and operational. Within each specific practice is a collection of responsibilities assigned to each practice area.

In general, ISM3 seeks to be comprehensive while making it easily aligned with the hierarchical structure of an organization. It advocates a lifecycle approach, compatible with other CMM approaches. As an organization improves its maturity, it will adhere to more practices in a more effective and efficient manner.

ISM3 generally borrows from several other frameworks available, such as ISO/IEC 17799. For this reason, the framework is generally comprehensive and usable. However, due to the similarity with these other frameworks, ISM3 also suffers from a degree of obscurity as it is not an internationally recognized standard, nor has it received the considerable amount of support or attention that other frameworks, like COBIT, have received.

ISM3 does rely on certain assumptions. For example, it needs an Information Security Management System (ISMS) to have been implemented previously. This perilously binds the framework to another framework, such as ISO/IEC 17799, that provides guidance on actually implementing an ISMS. Unfortunately, this begs the question "Why would I deploy ISM3 if I've already deployed 17799?" The answer is "I don't know." To do so would be to deploy a framework onto a framework. Doing this does not seem particularly useful or efficient.

Where ISM3 does seem to represent value is as a lightweight method for testing a deployed ISMS to ensure effectiveness. In the end, however, one has to believe that the amount of effort required to deploy ISM3 would outweigh the overall value that could be derived from its implementation.

5. INFOSEC Assurance Capability Maturity Model

Official Name: INFOSEC Assurance Capability Maturity Model

Abbreviation(s): IA-CMM

Primary URL: http://www.iatrp.com/iacmm.cfm

Classification: Framework

Status: Complete, Construction

Stated Objective: "The IA-CMM architecture is designed to enable a determination of an organization's process maturity for performing IAM assessments and IEM evaluations." [*35, p.25*]

Analysis: The IA-CMM is classified here as a framework because it provides specific guidance for implementation. While the CMM includes the word "model," in this case the associated guidance is far more specific than a model, by the definition used here, should be. Furthermore, IA-CMM binds itself to a narrow topic in INFOSEC Assurance.

The IA-CMM [*35*], in v3.1, has evolved to become a framework for INFOSEC Assurance. Based on the SSE-CMM (ISO/IEC 21827), IA-CMM defines six levels of capability maturity resulting from testing nine process areas. Those process areas are:

- Provide Training
- Coordinate with Customer Organization
- Specify Initial INFOSEC Needs
- Assess Threat
- Assess Vulnerability
- Assess Impact
- Assess INFOSEC Risk

- Provide Analysis and Results
- Manage INFOSEC Assurance Processes

The purpose of a capability maturity model is to define a method by which to select and implement process improvement strategies. This philosophy is based in large part on the groundbreaking work of W. Edward Deming and seeks to create a learning organization that is capable of improving predictability, control, and process effectiveness.

For those organizations that have already invested in CMMi or similar initiatives, then implementation of the full IA-CMM may be worthwhile. Even if an organization has not deployed a CMM previously, there are useful lessons to derive from a study of IA-CMM. In particular, the nine process areas of the IA-CMM provide a general framework that could be applied to an INFOSEC program within a given organization.

The downsides of the IA-CMM are that it is a CMM-based framework and it is focused exclusively on INFOSEC Assurance. In the first case, there are many published pros and cons associated with use of a CMM model, ranging from testing not having wide enough scope to the philosophy not being compatible with American business culture. In the former case, INFOSEC Assurance, as defined by IA-CMM, does not include many key aspects of INFOSEC, such as incident response, business continuity, or secure communications.

6. ISF Standard of Good Practice

Official Name: The Information Security Forum Standard of Good Practice

Abbreviation(s): IFS Standard, The Standard

Primary URL: http://www.isfsecuritystandard.com/

Classification: Framework

Status: Complete, Construction

Stated Objective: "The Standard is designed to present organisations with a challenging but achievable target against which they can measure their performance." [*13, p.1*]

Analysis: The ISF Standard of Good Practice [*13*] is a culmination of research and membership feedback that has been developed by the ISF. It attempts to address information security from a business perspective by focusing on the arrangement necessary to keep business risks associated with critical information systems under control.

ISF describes the benefits of implementing the Standard as helping organizations to:

- "move towards international best practice
- manage the breadth and depth of information risk
- build confidence in third parties that information security is being addressed in a professional manner
- reduce the likelihood of disruption from major incidents
- fight the growing threats of cybercrime
- comply with legal and regulatory requirements
- maintain business integrity." [*13, p.7*]

The Standard is divided into five aspects that each contains practice statements for implementation. The five aspects are: Security Management (enterprise-wide), Critical Business Applications, Computer Installations, Networks, and Systems Development. The framework is organized such that each aspect is defined at a high level, matrixed to common information security practices, and then fully specified.

Overall, the Standard represents a very valuable cookbook of "international best practices" that can be leveraged by an organization in deploying any number of other frameworks. As a standalone framework, however, the Standard is not overly

useful. Instead, the Standard would be best used as a supporting document when deploying another framework, such as COSO or ISO/IEC 17799. The best practices described could be used to assist in the decision-making process when defining and evaluating controls.

7. ISO 17799 / ISO 27001

Official Name: ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management

ISO/IEC FDIS 27001:2005 Information technology – Security techniques – Information Security Management Systems – Requirements

Abbreviation(s): ISO 17799, x7799, ISO 27001, FD-27001, BS 7799, BS 7799-1:2005, BS 7799-2, BS 7799-2:2005

Primary URL: http://www.iso.org/

Classification: Framework

Status: 17799: Complete, Construction
27001: Construction

Stated Objective: 17799: To be a "practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities." [*17, p.1*]

27001: To specify "the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks." [*18, p.1*]

Analysis: ISO/IEC 17799 was originally released as a Standard in 2000 (1995 for the BSi equivalent) and continues to be updated every few years. Prior to the 2005 release, the most current version had been released in 2000. As stated above, the goal of

17799 is to provide a guideline for developing effective, documented security management practices, contributing to the development, implementation, and maintenance of an Information Security Management System (ISMS). 17799 was derived from BS 7799.

ISO/IEC FDIS 27001 is a final draft standard based on BS 7799-2, which provides the general guidance necessary for establishing an ISMS. Where 17799 provides the code of practice for information security management, 27001 sets down the requirements for implementing an ISMS, as well as, providing an audit baseline for use in testing an ISMS. In other words, these documents taken together provide the entire method for building an ISMS and progressing to the point of receiving certification for an ISMS.

Both of these standards have been classified here as frameworks because they address an overall topic conceptually and then proceed to deliver practice statements toward implementation of that concept.

The ISMS approach described within these frameworks results in a truly comprehensive security management approach that starts with the business, identifies and analyzes risk, and builds an entire program for addressing that risk. In this sense, the approach is very similar to COSO.

Where COSO and 17799/27001 differ is in the focus. As mentioned above, COSO focuses on enterprise risk management and contains practice statements for implementing that approach, whereas 17799/27001 focuses on developing a comprehensive system for managing information security. These concepts are very similar, in that they both focus on business risk, but they come at the problem from nuanced angles. 17799/27001 looks at the organization as a whole, walks through requirements for an ISMS, maps those requirements into the business, and seeks to adapt the ISMS itself to the business's operations. COSO also looks at the business, but appears to have a slightly more

rigid structure for implementation. The various CMMs have even more rigid structures that essentially require the business to change its operations to match the framework.

17799/27001 is very beneficial to an organization because of its comprehensive approach. This approach has become even more comprehensive in the 2005 release, filling in some holes that previously existed (such as around incident response management). If taken seriously and implemented thoroughly into the business, 17799/27001 can have the strong effect of improving the performance of the entire organization. Similar to the older IT alignment models of the 1980s and 1990s, 17799/27001 seeks to create a malleable organization that can detect and respond to change and risk.

On the other side of the scale, 17799/27001 requires significant buy-in to be properly implemented. Moreover, having been developed in the UK initially, it represents a way of thinking that is not completely compatible with American business psychology. This downside is very similar to that suffered by the CMM derivatives.

The good news is that ISO has established a track record of success with the 900x series of standards within manufacturing. These successes can be translated into other product and services industries. However, it will take a compelling argument to finally turn the corner.

One such compelling argument is in the increasing amount of regulations, as discussed below. For example, if an ISMS is properly implemented with full documentation and working processes, it can be used as a shield to defend against the ever-changing regulatory environment. Furthermore, key frameworks like COBIT have been mapped to 17799/27001 such that routine audits by external audit firms should become more efficient; accomplishing the goals underlying COBIT. Additionally, a 17799/27001 deployment would

necessarily impact the overall organization. Implemented properly, 17799/27001 will improve organizational performance in a positive way.

8. ITIL / BS 15000

Official Name: ITIL: Information Technology Infrastructure Library
BS 15000: Information Technology Service Management Standard

Abbreviation(s): ITIL, BS 15000, ITSM

Primary URL: http://www.itil.co.uk/
http://www.bs15000.org.uk/

Classification: Framework

Status: Complete

Stated Objective: The primary focus of ITIL and BS 15000 is the successful implementation of IT Service Management.

Analysis: *Note*: *This section is provided for completeness, but the analysis performed is minimal. Adequate documentation describing ITIL could not be found for free on the Internet and the author did not have a budget for purchasing copies of the standard.*

ITIL is described as a standard for developing and deploying an IT Service Management (ITSM) framework. It is a library of practices that are to be used for such a purpose. It is comprised of seven sets of guidance: Managers Set, Service Support, Service Delivery, Software Support, Networks, Computer Operations, and Environmental. Though originally developed by the UK Government, it has seen fairly broad adoption throughout Europe.

BS 15000 is a British Standard based extensively on ITIL. It is broken into two parts. Part 1 provides guidance for implementing an ITSM system, while Part 2 provides assistance for organizations seeking

to be audited against Part 1, or that are going through an improvement cycle.

These works appear to be geared toward adoption by IT organizations with the overall goal of creating a service management framework. As such, these methods are perhaps closest in relation to COBIT, but yet very different from it. The commonality being the IT focus, the disparity being controls versus service management.

For more information, please visit the primary URLs provided above. The British Standards Institute (BSi) is probably the best source for receiving direct information and instruction.

9. New Basel Capital Accord (BASEL-II)

Official Name: International Convergence of Capital Measurement and Capital Standards: A Revised Framework

Abbreviation(s): BASEL-II, New Basel Capital Accord

Primary URL: http://www.bis.org/

Classification: Framework

Status: Complete

Stated Objective: To "preserve the integrity of capital in banks with subsidiaries by eliminating double gearing." [*5, p.7*]

Analysis: BASEL-II [*5*] is provided here for completeness. It is a framework targeted specifically at holding companies that are the parent of any international bank. As stated above, the purpose is to preserve the integrity of capital.

BASEL-II uses three pillars. The first pillar defines minimum capital requirements. The second pillar defines the supervisory process. The third pillar defines market discipline.

The primary applicability of this framework to

information security appears to fall under the categories of operational risk, supervisory review, and disclosure requirements. These requirements underscore the need to run a tight ship fully above board to prevent any one entity from becoming destabilized and having the greater effect of destabilizing other entities.

This framework has significantly limited applicability within the information security context. Unless your organization is involved in international banking, BASEL-II is probably not of concern. However, if your organization is involved in international banking, or a related undertaking, then you will probably need to become familiar with the directives provided.

For more information, please consult the URL provided above.

10. NIST SP 800-14

Official Name: National Institute of Standards and Technology, Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

Abbreviation(s): 800-14, NIST 800-14, SP 800-14

Primary URL: http://www.nist.gov/

Classification: Framework

Status: Complete

Stated Objective: To provide "a baseline that organizations can use to establish and review their IT security programs." [*33, p.1*]

Analysis: Published in 1996, NIST SP 800-14 [33] provides a very sound basis for the establishment of an IT security program. While the sheer age of the document might lead one to conclude that it is obsolete, nothing could be farther from the truth.

Many of the references within the document are now outdated, but the overall concepts and practice statements are still applicable today.

Nonetheless, familiarity with and use of this framework is only recommended from an historical perspective. Given its relation in time to the original publishing of BS 7799, one can clearly see commonality, and would probably rightly conclude that current versions of ISO/IEC 17799 supersede this effort.

800-14 defines eight generally accepted system security principles. Those principles are:

- Computer Security Supports the Mission of the Organization
- Computer Security is an Integral Element of Sound Management
- Computer Security Should Be Cost-Effective
- Systems Owners Have Security Responsibilities Outside Their Own Organizations
- Computer Security Responsibilities and Accountability Should Be Made Explicit
- Computer Security Requires a Comprehensive and Integrated Approach
- Computer Security Should Be Periodically Reassessed
- Computer Security is Constrained by Societal Factors

In addition to the eight principles, the framework goes on to define and describe fourteen (14) IT Security Practices. Those practices are:

- Policy
- Program Management
- Risk Management
- Life Cycle Planning
- Personnel/User Issues
- Preparing for Contingencies and Disasters
- Computer Security Incident Handling
- Awareness and Training
- Security Considerations in Computer

Support and Operations
- Physical and Environmental Security
- Identification and Authentication
- Logical Access Control
- Audit Trails
- Cryptography

In general this framework is more comprehensive from the infosec standpoint than many other frameworks described herein. Any individuals or organizations wishing to create a new model, framework, or methodology would do well to study the structure and approach of this framework to learn how to create a durable product.

11. Systems Security Engineering Capability Maturity Model

Official Name: Systems Security Engineering Capability Maturity Model

Abbreviation(s): SSE-CMM, ISO/IEC 21827

Primary URL: http://www.sse-cmm.org/

Classification: Framework

Status: Complete, Deprecated

Stated Objective: "The SSE-CMM is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are the Information Technology Security (ITS) domain." [*19, p.1*]

Analysis: Of all the CMM derivatives discussed within this paper, the SSE-CMM [*19*] was the most difficult to classify. At face value, it may belong under the classification of model, and indeed would have been, had it not digressed into specifying practices for implementation. Chapters 5-7 of the SSE-CMM are devoted to providing testable practices that can be used in assessing a maturity level. As such, SSE-CMM is classified as a framework.

The SSE-CMM is a general framework for implementing security engineering within an organization; preferably in conjunction with other engineering CMMs. SSE-CMM builds on the work of Deming much as other CMMs have done, focusing on process definition and improvement as a core value.

Taking this process improvement approach, SSE-CMM looks at the occurrence of security defects, or incidents, and seeks to identify the flaw in the related process so as to remediate the flaw, thus removing the overall defect. In order to achieve improvements in processes, those processes must be predictable, with expected results. Furthermore, controls must be defined and understood surrounding those processes. Finally, efforts should be made to improve the overall effectiveness of processes.

Section 2.3 of [*19*] provides a good overview of some common misunderstandings about SSE-CMM specifically, and which apply in general to CMMs.

SSE-CMM is a very strong, well-tested framework for integration into an engineering-oriented organization. If your organization performs engineering, such as through product development, then use of SSE-CMM, particularly in combination within other CMMs, would be very valuable.

However, given the engineering focus, SSE-CMM is not a good match for service organizations that are not organized around an engineering function. While SSE-CMM certainly has key lessons to teach in terms of managing information security holistically, those lessons will be difficult to implement outside of an engineering context.

The CMM approach in general, as based on the work of Deming, is very sound, yet very foreign to American business culture. Deming believed in starting with a statistical analysis of processes, and then using those statistics to isolated defects within those processes, toward the end-goal of gaining

better insight into processes and to foster an environment of continuous quality improvement with respect to processes.

Even if an engineering organization has started down a non-CMM path (such as Six Sigma), the SSE-CMM could provide value to the organization. For those organizations that are already leveraging a CMM approach, then the addition of SSE-CMM to the mix should be relatively straight-forward and could yield perceptible results in a short time period.

Methodologies

The following seven (7) methods have been determined to provide specific guidance toward implementation or execution of a specific task. Each method is classified as a methodology.

1. INFOSEC Assessment Methodology

Official Name:	INFOSEC Assessment Methodology
Abbreviation(s):	IAM
Primary URL:	http://www.iatrp.com/iam.cfm
Classification:	Methodology
Status:	Complete, Construction
Stated Objective:	To provide a method that "can be used as a standardized baseline for the analysis of the INFOSEC posture of... automated information systems." [*36, p.M1-3*]
Analysis:	IA-CMM, as described in III.C.5, is underpinned by three levels of testing. IAM represents the methodology for “Level 1: Assessments” under the "Vulnerability Discovery Triad." As such, IAM is focused on providing a high-level assessment of "a

specified, operational system for the purpose of identifying potential vulnerabilities." [36, M1-8] As part of the reporting through this methodology, recommendations for remediation are provided.

IAM is subdivided into three phases: Pre-Assessment, On-Site Activities, and Post-Assessment. The Pre-Assessment phase is intended to develop a general understanding of customer needs, identify target systems, and establish the "rules of engagement" for the assessment. Pre-Assessment concludes with a written assessment plan.

The On-Site Activities phase represents the primary thrust of IAM in that it takes the results of the Pre-Assessment Phase, validates those results, and performs additional data gathering and validation. The result of this phase is a report of initial analysis.

Finally, the Post-Assessment phase concludes the IAM by pulling together all the details from the previous two phases, combining them into a final analysis and report.

IAM training is generally broken into four (4) modules. The first module provides a background for and overview of IAM. The subsequent three (3) modules each focus on a phase, starting with Pre-Assessment, moving on to On-Site Activities, and concluding with Post-Assessment.

This methodology is generally high-level and non-technical. In comparison, IAM is roughly comparable to the performance of a full SAS 70 Type II assessment. The testing begins with paper-based definitions, and then moves into a phase of basic validation of those definitions, without doing major technical testing.

As it addresses Level 1 of the “Vulnerability Discovery Triad,” IAM does not compare directly to IEM, but is instead the first step of the overall process, leading up to IEM in Level 2.

IAM may best be compared to OCTAVE[SM] below in that it is a non-technical assessment of vulnerabilities and, by extension, risk.

2. INFOSEC Evaluation Methodology

Official Name: INFOSEC Evaluation Methodology

Abbreviation(s): IEM

Primary URL: http://www.iatrp.com/iem.cfm

Classification: Methodology

Status: Complete, Construction

Stated Objective: To provide a method for technically assessing vulnerability in systems and to validate the actual INFOSEC posture of those systems. [*37, p.M1-22*]

Analysis: The IEM [*37*] is a companion methodology to IAM, fitting under the overall umbrella of the IA-CMM framework, but targeting Level 2 of the "Vulnerability Discovery Triad." As such, IEM works hand-in-glove with IAM, matching the overall process format almost exactly. The key differentiation between IAM and IEM is that the IEM performs actual hands-on assessment of systems in order to validate the actual existence of vulnerabilities, as opposed to the IAM's result of document possible vulnerabilities in those systems.

Similar to the IAM, the IEM is divided into three phases: Pre-Evaluation, On-Site, and Post-Evaluation. The Pre-Evaluation phase begins with taking the IAM Pre-Assessment report as input and then coordinating the rules of engagement for conducting technical evaluation of the systems under target. This phase concludes with a Technical Evaluation Plan.

The On-Site phase of the IEM then represents the bulk of the hands-on technical work, performing various discoveries, scans, and evaluations. All

findings are manually validated to ensure accuracy.

Finally, the Post-Evaluation phase concludes the methodology in a manner similar to the IAM by pulling together all data generated, putting it into a final report that details findings, recommendations, and a security roadmap. The IEM closes with customer follow-up and support.

It is interesting to note that the IEM can be conducted either following, or in conjunction with, the IAM. In contrast to the IAM, the IEM will perform actual testing of systems, validating findings manually to ensure accuracy of reporting. The deliverable from the IEM is more significant and comprehensive than the IAM report, providing analysis, matrices, and reporting of findings.

3. ISACA Standards for IS Auditing

Official Name: Information Systems Audit and Control Association Standards for Information Systems Auditing

Abbreviation(s): ISACA IS Auditing Standards

Primary URL: http://www.isaca.org/

Classification: Methodology

Status: Complete, Construction

Stated Objective: To provide a comprehensive standard for the performance of information systems (IS) auditing.

Analysis: ISCA describes its Standards for IS Auditing [*14*] as "The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community." [*14, p.6*] As such, the IS Auditing Standards (ISAS) represent a very detailed methodology for the performance of IS auditing tasks.

ISAS leverages ISACA's other primary work, COBIT, in providing a common set of guidance and

practices to IS auditors. It is subdivided into eight standards, each of which contains one or more guidelines. The eight standards are Audit Charter, Independence, Professional Ethics and Standards, Competence, Planning, Performance of Audit Work, Reporting, and Follow-Up Activities.

These standards, guidelines, and associated procedures are revised on an ongoing basis, continuously morphing to match the current IS and regulatory environment. The guidance provided within the ISAS runs the gambit of auditing responsibilities and is best targeted to an IS auditor audience.

If your organization is subject to annual financial and IS auditing, then having auditors who are familiar with this methodology, as well as the COBIT framework, is an absolute must.

4. OCTAVE℠

Official Name: Operationally Critical Threat, Asset, and Vulnerability Evaluation℠

Abbreviation(s): OCTAVE℠, OCTAVE

Primary URL: http://www.cert.org/octave/

Classification: Methodology

Status: Complete

Stated Objective: To be "a self-directed information security risk evaluation." [2, p.5]

Analysis: The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠) [*1, 2, 3, 4*] methodology is, in a nutshell, a high-level risk assessment methodology that balances foci of operational risk, security practices, and technology. The methodology is organized around a three basic phases. They are:

- Phase 1: Build Asset-Based Threat Profiles

- Phase 2: Identify Infrastructure Vulnerabilities
- Phase 3: Develop Security Strategy and Plans

Overall, OCTAVE is a risk-based assessment and planning methodology that focuses on "strategic, practice-related issues" [*1, p.3*] Per the approach overview, "The OCTAVE approach is driven by two of the aspects: operational risk and security practices. Technology is examined only in relation to security practices, enabling an organization to refine the view of its current security practices." [*1, p.3*]

The suite of documentation comprising OCTAVE provide very extensive guidance for the overall process, describing how to create and coordinate a cross-functional analysis, develop threat profiles, identify vulnerability, and develop an over security strategy and plan; all inline with the three main phases.

Given adequate time and resources, an organization wishing to conduct a high-level risk assessment for their organization, such as to determine an overall strategic plan, would be well-advised to consider the OCTAVE methodology.

In contrast to other high-level assessment methodologies, such as IAM, OCTAVE is marked by its nature of being self-directed. Instead of bringing in an external organization to perform the assessment for you, you would instead hire an OCTAVE expert to train and shepherd your analysis team in the process.

5. OSSTMM

Official Name: Open Source Security Testing Methodology Manual

Abbreviation(s): OSSTMM

Primary URL: http://www.isecom.org/osstmm/

Classification: Methodology

Status: Incomplete, Construction

Stated Objective: To provide "a professional standard for security testing in any environment from the outside to the inside." [*11, p.9*]

Analysis: The Open Source Security Testing Methodology Manual [11, 12] is best described in its own words:

> *"This is a document of security testing methodology; it is a set of rules and guidelines for which, what, and when events are tested. This methodology only covers external security testing, which is testing security from an unprivileged environment to a privileged environment or location, to circumvent security components, processes, and alarms to gain privileged access. It is also within the scope of this document to provide a standardized approach to a thorough security test of each section of the security presence (e.g. physical security, wireless security, communications security, information security, Internet technology security, and process security) of an organization. Within this open, peer-reviewed approach for a thorough security test we achieve an international standard for security testing to use as a baseline for all security testing methodologies known and unknown."* [*11, p.10*]

In general, the document provides an excellent primer for security testing. It was developed taking many forms of legislation into consideration from countries including Austria, the US, Germany, Spain, Canada, the UK, and Australia. Additionally, it builds on best practices from sources such as ITIL, ISO 17799, NIST standards, and MITRE. It also has a companion manual that focuses on wireless system testing.

The document is labeled here as "Incomplete"

because several sections of the manual indicate such a status. It's possible that the manual is, in fact, complete, but not available for free distribution on the Internet. Version 2.1 of the manual was reviewed for this paper, though the primary URL above indicates that version 3.0 is due out momentarily. Furthermore, it is noted that updates to the manual are not posted publicly on the site, but instead are only distributed to ISECOM members.

Any individual or organization wishing to develop a security testing methodology would benefit greatly from gaining familiarity with and understanding of this manual. The fact that it has coordinated best practices and legislation from so many separate sources alone makes it a highly valuable resource for the security tester.

6. Security Incident Policy Enforcement System

Official Name: Security Incident Policy Enforcement System

Abbreviation(s): SIPES

Primary URL: http://www.isecom.org/projects/sipes.shtml

Classification: Methodology

Status: Incomplete

Stated Objective: To provide a methodology for defining and implementing a Security Incident Policy Enforcement Systems.

Analysis: This methodology is listed for completeness. However, due to its status as an "Incomplete" work that has not demonstrated progress over the past two years, it is presumed that work has not continued and that this methodology is, in fact, obsolete

The Security Incident Policy Enforcement System (SIPES) [*32*] draft represents a relatively abstract approach to addressing the problem of incident response management. The paper starts by de-

conflicting the definition of failure within IT systems and then proceeds to build its "state-full" methodology. The underlying approach is to discuss security state and those points where states change. Using that dynamic basis, they then move into the argument for incident policy enforcement, with several sidebars into what each of these terms means.

The rest of the paper is then dedicated to the process of defining and creating a SIPES. The paper is generally abstract and conceptual in nature, but it describes an overall methodology for performing assessments toward the end-goal of creating a SIPES.

7. SAS 70

Official Name: Statement on Auditing Standards Number 70

Abbreviation(s): SAS 70

Primary URL: http://www.sas70.com/

Classification: Methodology

Status: Complete, Construction

Stated Objective: To be an internationally recognized auditing standard.

Analysis: The basis for this analysis is the information available at the above URL, combined with personal experience. Due to the nature of SAS 70 really being a compendium of Statements of Auditing Standards from the American Institute of Certified Public Accountants (AICPA), it should be presumed that the specifics of this methodology are shifting on a regular basis.

Prior to the emergence of the Sarbanes-Oxley Act of 2002 and the decision by the Big 4 audit firms to generally follow COBIT for the purposes of audit and compliance examinations, the SAS 70

methodology was the gold standard for evaluating an organization's documented and implemented controls.

The SAS 70 is generally divided into two categories: Type I and Type II. The Type I audit is primary a paper-based audit that reviews documented controls and works with an organization through remediation efforts to produce documented controls that are reasonable, adequate, and effective.

The Type II audit adds additional steps beyond the Type I review. In particular, systems are checked for compliance with the documented controls. Tests are also conducted to determine the effectiveness of the controls defined.

In general, the SAS 70 will be required of organizations by third parties to demonstrate a general wherewithal as it pertains to documenting and implementing controls. Third parties are often interested in seeing such an audit performed in cases where partnerships or being formed, or where mergers and acquisitions are involved.

The SAS 70 methodology itself is a collection of auditing standards developed and published by the AICPA. This list of standards is not finite, but in continual flux.

In terms of duration, an organization should expect that a Type I audit will last a minimum of 3-6 months and as long as 18 months. Duration of the audit relates to the quality of documented controls and effectiveness of their implementation. A Type II audit can take as much as an additional 6-18 months beyond the Type I audit.

Ultimately, in the SOX environment today, no publicly traded company should need to have a SAS 70 performed since SOX requires controls to be documented, implemented, and effective. SOX requires that the annual audit include statements of control effectiveness. Where the SAS 70 may add

> value is in preparing for the annual SOX audit as a checkup to ensure that an organization has adequately documented controls and effectively implemented them.

MEETING US-CENTRIC REGULATIONS

A common challenge facing organizations today is meeting the myriad regulations from industry and legislature. This section of the Literature Review seeks to provide an overview of some common regulations facing organizations today, with particular focus on the common themes that must be addressed. After establishing this regulatory baseline, a brief discourse is entered into discussing which – if any – model, framework, or methodology may be useful in meeting these requirements.

Regulatory Overview

Whether looking at the Sarbanes-Oxley Act of 2002 (SOX), The Gramm-Leach-Bliley Act of 1999 (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standards (as adopted by the Visa CISP and MasterCard SDP program), or FTC, NCUA, and SEC regulations, as well as, any State-originating regulations like California SB-1386, it becomes clear that none of the models, frameworks, or methodologies described above will ensure full compliance by default. However, certain methods can help position a company to demonstrate due diligence and address key practices involved in compliance, audit, and governance.

Rather than provide a restatement of a handful of common regulations, which can be found in droves via a simple Google search, it is instead instructive to look at the core requirements affected by these regulations. A quick review of the key provisions in SOX,

GLBA, HIPAA, PCI DSS, and other regulations reveals an interesting trend. For the most part, these laws require that organizations use a common sense approach (to security practitioners, anyway) in protecting data, disclosing privacy policies, and governing their business to ensure reliability in financial reporting.

To give an example, both GLBA and HIPAA have very similar provisions on privacy and protection of non-public personal information. In both cases, organizations subject to the regulations are required to disclose their privacy policies to customers up front. This disclosure must describe how personal data is handled and inform customers of any situations where the organization may disclose data to third parties. Additionally, both regulations require that common sense measures, similar to those required by PCI DSS (described next), be implemented on systems containing protected data.

As indicated, the PCI DSS, as adopted by Visa and MasterCard, requires that organizations implement very common sense information security measures. Whereas extensive guidance is provided regarding how to implement those security measures, there are really only six (6) high-level categories that map to twelve (12) required practices. The categories and practices are as follows:

1. Build and Maintain a Secure Network
    - Requirement 1: Install and maintain a firewall configuration to protect data
    - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data
    - Requirement 3: Protect stored data
    - Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks
3. Maintain a Vulnerability Management Program
    - Requirement 5: Use and regularly update anti-virus software
    - Requirement 6: Develop and maintain secure systems and applications

4. Implement Strong Access Control Measures
    Requirement 7: Restrict access to data by business need-to-know
    Requirement 8: Assign a unique ID to each person with computer access
    Requirement 9: Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks
    Requirement 10: Track and monitor all access to network resources and cardholder data
    Requirement 11: Regularly test security systems and processes.
6. Maintain an Information Security Policy
    Requirement 12: Maintain a policy that addresses information security

Source: [39]

Finally, the only piece of this puzzle that is missing is the piece represented by the Sarbanes-Oxley Act of 2002, or SOX for short. SOX came about as a result of the Federal Government uncovering illegal accounting practices at major U.S. corporations (Enron, WorldCom) that resulted in defrauding stockholders. Despite the fact that adequate legislation was already on the books banning the type of practices found, the U.S. Congress decided to publish a new Act that reinforced the notion that companies must take care in assuring the reliability of their financial reporting, including to the extent of implementing internal controls and assessing those controls on an annual basis to determine effectiveness.

One key change represented by SOX was that top executives were now criminally liable for inaccurate financial reporting. Furthermore, the Act requires that companies annually assess the effectiveness of their internal controls, publishing a statement with their annual financial reporting that indicates the outcome of those assessments. Additionally, those statements of effectiveness are to be independently verified by the external auditor. Any discrepancies in reporting may result in legal action, and failure to implement and maintain effective controls may have a negative impact on the financial performance of the company, not to mention creating the potential for legal action by stakeholders.

The resulting rules defined by the American Institute of Certified Public Accountants (AICPA) and the Public Company Accounting Oversight Board (PCAOB) in relation to SOX required that public companies subject to the regulations document the framework used to conduct the mandatory assessment of internal controls effectiveness. Pertaining to Section 404 of the legislation, the COSO framework (initially the original guidance from 1987, and later the updated guidance discussed above) must be the basis for the required assessment.

Models, Frameworks, and Methodologies of Use

Before launching into a discourse on which models, frameworks, or methodologies may be useful in meeting the regulatory demands of today, let's first pause to recap the common themes contained within the various regulations. First, it is important to implement a comprehensive information security management program that defines policies, including the disclosure of a privacy policy to customers, defines internal controls, and includes statements of responsibility, such as that the program and its effectiveness are ultimately owned by executive management.

Second, the information security management program should implement commonsense security measures to protect data and systems. These measures should include maintaining information security policies (reiterated), building a secure network, protecting stored and transmitted data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks and systems, and maintaining a business continuity and disaster recovery program that plans for backup, recovery, and contingencies.

Finally, the entire program should be assessed on a regular basis. In particular, internal controls must be annually assessed to ensure effectiveness and to assure that data is properly protected. These assessments can be conducted internally, but must be verified externally, especially in the case of public companies.

The question at hand, then, is what model, framework, or methodology might address all of these requirements in a suitable manner. In short, the answer is almost soundly "none." However, there are a couple exceptions. For instance, ISO/IEC 17799 is designed such that it can be customized to meet the requirements of the business, including those external drivers represented by the regulator environment. SSE-CMM may also be a tenable solution, having the same malleable qualities, but is generally limited to those organizations that leverage engineering processes. It should, however, be noted that SSE-CMM appears to be deprecated, lacking further support or development.

The COSO ERM framework may provide a good starting point for meeting these requirements. However, it is not enough on its own. It may be supplemented with COBIT, OCTAVE, IA-CMM, IAM, IEM, ITIL, or even ISO/IEC 17799. Alternatively, NIST SP 800-14 may be used as the basis for an infosec management program, bolstered by the ISF Standard of Good Practice.

From the standpoint of regular assessments, OSSTMM would be a good basis for organizations wishing to build their own assessment methodology. Alternatively, organizations could also build on the work of IA-CMM, IAM, and IEM.

What is very clear is that frameworks like COBIT will not address the full breadth of the regulator environment. Despite assertions made by the public accounting firms, the scope of COBIT is strictly limited to IT controls, and thus does not meet the broader infosec requirements stipulated by other regulations, such as PCI DSS, GLBA, HIPAA, or the NCUA. Whereas it may be convenient for internal audit groups to view the world through the lens of COBIT, it is not useful for the overall organization to commit too fully to implementation of COBIT. Ultimately, COBIT directly benefits the organizations peddling it, which also happen to be the organizations writing the rules requiring use of frameworks like COBIT.

From a broad standpoint, then, the only framework that holds the promise of meeting the majority of requirements is ISO/IEC 17799. Furthermore, since 17799 is by definition flexible, it can be customized in the short-term and long-term to meet the ever-changing regulatory landscape. Moreover, it can be mapped to, or integrate with, other frameworks and methodologies so as to round out information security management program. Finally, 17799 holds the distinct advantage that it would not require a major change in business philosophy, such as a CMM-based approach would entail.

LITERATURE REVIEW CONCLUSIONS AND SUMMARY

This Literature Review has provided an overview and analysis of nineteen (19) models, frameworks, and methodologies. A taxonomy was created that defined each of these categories. A model was defined as a high-level conceptual construct lacking practicability guidance. A framework was defined similarly to a model, but including more detail within the construct and supported by general practice statements for implementation. And, finally, a methodology was

defined as a focused construct that provided detailed guidance for implementation. The methods were classified as follows:

Models	Frameworks	Methodologies
McCumber Cube	COBIT	IAM
	Common Criteria	IEM
	COSO ERM	ISACA IS Auditing Standards
	ISM3	OCTAVE
	IA-CMM	OSSTMM
	ISF Standard	SIPES
	ISO 17799/27001	SAS 70
	ITIL/BS 15000	
	BASEL-II	
	NIST SP 800-14	
	SSE-CMM	

Of these methods, only a few were found to have general utility in providing the basis for an overall program (whether focused on risk management or information security management). Those programs include: COSO, ISO/IEC 17799/27001, ISM3, and SSE-CMM. Of these, COSO and 17799 represented the most viable options for building a program, and differed primarily in the overall focus of the approach. ISM3 holds promise, but only for those organizations that are capable of adapting to a CMM-based management approach

Beyond the general approaches, it was found that many methods have very tight foci, such as on IT. COBIT and ITIL/BS 15000 in particular suffer from this condition and, as such, prevent themselves from being useful in a broader context.

Some methods were also found to be bound by their intended audience. For example, BASEL-II is only intended for an international banking audience, while the ISACA IS Auditing Standards are addressed to an auditing audience. SAS 70 is also generally limited to an audit-oriented audience, though it is seeing broader use in light of the increasing regulatory environment.

Other methods were limited by their objectives. The Common Criteria, while interesting, has limited applicability as its primary mission is to provide a lingua franca for describing a product being evaluated. Similarly, besides being incomplete, SIPES had a focus on security incident policy enforcement.

Perhaps the most interesting result of this research is that only one method achieved classification as a model. This accomplishment is noteworthy because of its uniqueness. The reason the McCumber Cube was classified as a model was because it was truly generic, didn't get bogged down with specific direction for implementation, and was designed so as to withstand rigor. In contrast, other candidates, like COSO and ISO 17799, did not sufficiently compartmentalize themselves so as to establish a model, and then find a corresponding method for implementation. The IA-CMM is perhaps the closest example of nearly accomplishing this goal. Unfortunately, it too digresses into practice statements for implementation, despite being propped up by the IAM and the IEM.

From a usability standpoint, when measured against the regulatory environment, it was found that the targeted frameworks and methodologies could oftentimes meet specific regulations, but were not well adapted to address a large cross-section of requirements. In contrast, the broader frameworks, as well as the ISF Standard, represented works that could be broadly useful in addressing external requirements placed upon organizations.

Finally, it is useful to point out that there is no shortage of audit-related materials. Of the nineteen methods analyzed, three were directly related to the auditing field and another six had a significant focus on audit or assessment. In light of these findings, it is then not surprising how much confusion exists surrounding which approach is best suited to "securing" an organization.

Hopefully this research has helped shed light on this situation and will be a useful tool to individuals and organizations seeking to improve the maturity of their organizations while sufficiently addressing their regulatory burdens.

III. Research Method

The research method used in this effort leveraged both quantitative and qualitative approaches. First, data was collected exhaustively from every available source. Data collected included descriptions of information assurance models, frameworks, and methodologies; legislative and regulatory requirements for both public and private sector entities; and, case studies on the actual use of information assurance governance approaches. The data was parsed into conceptual elements and then brought together in an overarching framework. This framework was used as the instrument for qualitative interviews with subject matter experts. The interview data was analyzed to assess the framework.

Research Plan

The plan of research was comprised of three main phases: 1) Collection and documentation of information assurance methods; 2) Creation of an overarching information assurance method that harmonizes the key areas of enterprise risk management, operational security management, and audit management; and, 3) Validation of the overarching method by subject matter experts.

Phase 1: Collection and Documentation of Information Assurance Methods

The first phase of proposed research was to – as exhaustively as possible – identify models, frameworks, and methodologies that have been produced for purposes under the heading of information assurance. This initial phase provided the basis for later phases and is contained within the Literature Review above. In this phase, each identified approach was described in accordance with its self-contained documentation, classified according to a standard taxonomy, and afforded brief commentary describing assertions made about the use of the method.

This phase represents a useful contribution to industry, and thus has been made available as a standalone white paper for free dissemination to interested persons.

Phase 2: Creation of an Overarching Assurance Management Model

The second phase of research was to create, based on phase 1, a unified model that harmonized the key focus areas of enterprise risk management, operational security management, and audit management. This grouping of areas has been placed under the collective heading of information assurance management for the purposes of this research. The model is high-level in nature and allows for flexibility of use.

Phase 3: Validation of the Overarching Method by Subject Matter Experts

The final phase of the research involved soliciting subject matter experts for their opinions regarding the model developed in the previous phases. This approach was taken because it is impractical to test the implementation of the model in any experimental method. The experts were selected based on their education, background, and membership in the information assurance profession. Their opinions were elicited to test the following hypotheses:

H1a: Organizations that adopt a unified approach to information assurance will be more efficient than organizations that do not adopt a unified approach.

H1b: Organizations that adopt a unified approach to information assurance will be more effective than organizations that do not adopt a unified approach.

H1c: Organizations that adopt a unified approach to information assurance will manage risk better than organizations that do not adopt a unified approach.

H1d: Organizations that adopt a unified approach to information assurance will optimize their operations better than organizations that do not adopt a unified approach.

This validation approach was organized as follows:

1. Identify subject matter experts (SMEs).
2. Solicit SME participation in validation process.
3. Present phase 1 and phase 2 findings to SMEs for review.

4. Survey and interview SMEs to identify and discuss opinions on the results of phases 1 and 2.
5. Documentation of survey results and incorporation of results in the thesis.

IV. Analysis

In performing the literature review, efforts were made to identify a single overarching model that incorporated the three key aspects of assurance management (enterprise risk management, operational security management, and audit management) into a single, harmonized approach. No model meeting these requirements was identified. Thus, research turned to creating such a model. This section presents the model created, describing its key components.

Before launching into a description of the Total Enterprise Assurance Management (TEAM) model, it is important to understand terms and phrases used within this research. Following are some quick definitions of key terms and phrases. Please note that the competency areas, in particular, will be further defined and discussed later in this document.

- Model: An abstract, conceptual construct that represents processes, variables, and relationships without providing specific guidance on or practices for implementation. The term is used throughout this research to denote approaches that are defined at a high level without getting into specific, detailed guidance on implementation.
- Framework: A fundamental construct that defines assumptions, concepts, values, and practices, and that includes guidance for implementing itself. Used with this research, the term denotes an approach that is documented with adequate detail for direct implementation.
- Methodology: A targeted construct that defines specific practices, procedures, and rules for implementation or execution of a specific task or function. Typically, methodologies can be directly executed to accomplish the specific task against which the methodology is defined.

- Enterprise Risk Management (ERM): In the context of this research, enterprise risk management is the competency area within business practices that defines business requirements and receives feedback from internal risk assessments and both internal and external audit reports, setting direction and strategy for the organization with respect to control, mitigation, and acceptance of risk. The ERM competency could be construed as pertaining to "security risk management," or it could be treated more broadly to speak to risk management in general.
- Operational Security Management (OSM): This competency area is focused on the implementation of security countermeasures throughout the enterprise. Some organizations may think of this as the information security management area of an organization, or associate it with practices such as Information Security Management Systems (from ISO 17799/27001) or a security-oriented capability maturity model, such as represented by the Information Security Management Maturity Model (ISM3).
- Audit Management (AuM): The functional competency area of audit management is traditionally the domain of internal (and possibly external) auditors. Within this context, these functions are lumped together in a specific zone of responsibility in order to establish and maintain independence from the business and operations.
- Assurance Management (AsM): Within this research, the phrase "assurance management" has been selected as a matter of convenience. Keyword overloading has occurred with many phrases, such as those described above. This phrase was selected because it is not as overloaded as other phrases (such as "information security management") and because it can carry a broad enough definition to be used

as an umbrella term for the key competency areas of enterprise risk management, operational security management, and audit management.

Model Overview

The following diagram provides an overview of the basic construct of the Total Enterprise Assurance Management (TEAM) model.

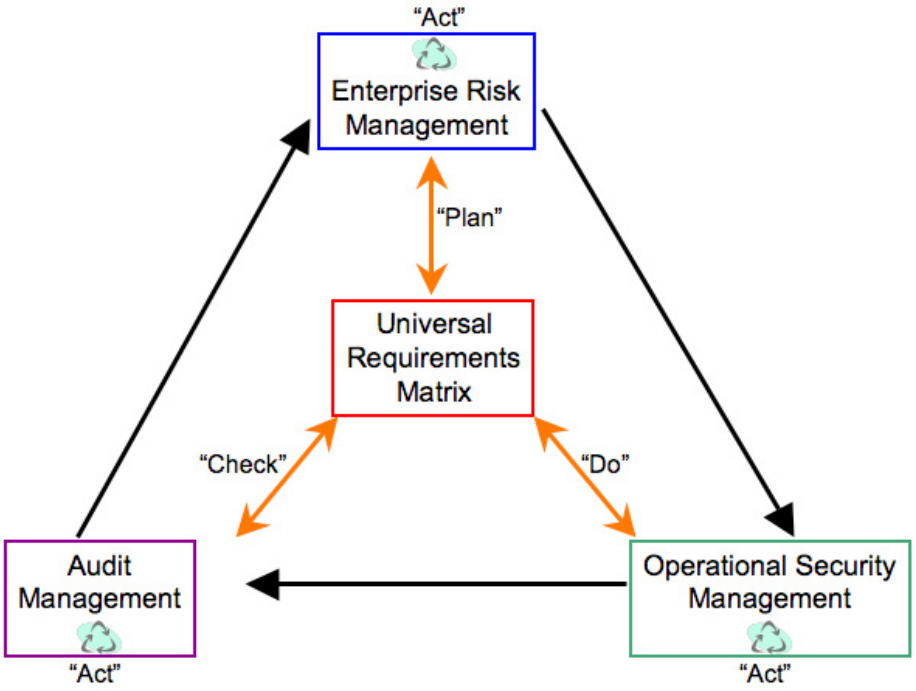

Figure 2: Basic TEAM Model

As will be discussed later, this model can be enhanced to include an overlay for a policy framework and to enforce independence with the audit function.

The TEAM model is based in part on the generic ISO lifecycle approach of Plan-Do-Check-Act (PDCA). It is not focused solely on IT security or service management, but instead

looks at assurance management from a high-level perspective, providing an overall approach for identifying business requirements, security requirements, and control objectives; implementing those requirements and controls; and auditing for discrepancies in the implementation, as well as in the definition of, the requirements and controls.

The model does, however, deviate from strict conformance to PDCA in that it relies on embedded lifecycles. As such, the top-level lifecycle is represented primarily as Plan-Do-Check, with the "Act" step distributed across each of the three competencies. These competencies, in turn, should implement an iterative lifecycle approach internally. For example, if each competency were to implement a PDCA lifecycle internally, the overall flow would look like: Plan (Plan-Do-Check-Act) – Do (Plan-Do-Check-Act) – Act (Plan-Do-Check-Act). In this sense, the TEAM model has allocated a full PDCA lifecycle to each competency as a required "Act" of the phase.

The TEAM model is comprised of four key components in addition to the overall lifecycle approach. Those components are the Universal Requirements Matrix (URM) and the three competency areas (Enterprise Risk Management, Operational Security Management, and Audit Management). Being primarily driven by a risk management approach, the model is designed to start with the ERM phase, progress to OSM, and then conclude with AuM, which in turn feeds back into ERM. The key is that these phases all circulate around the central axis of the URM.

The Universal Requirements Matrix (URM)

The Universal Requirements Matrix (URM) is the central piece of the TEAM model, and the single-most important component that an enterprise should implement. The role of the URM

is to combine business requirements – including operational requirements, business continuity requirements, and baseline security practices – with external requirements to which the enterprise must conform using a common language, or taxonomy. Rather than taking a piecemeal approach to defining and communicating requirements – as has been witnessed in response to the recent wave of regulations (e.g., Sarbanes-Oxley, Payment Card Industry Data Security Standards) – it is preferable to establish a single set of requirements that map out to each external requirement function.

One possible approach to implementing the URM may be to use a table that defines the requirement, mapping it to its external requirements. For example:

Requirement	Guidance	SOX	GLBA	PCI DSS
(…)	(…)	√ (ref.)		√ (ref.)

It should be noted and stressed here that the URM should start with business requirements. External requirements should only be considered after business requirements are defined. Whereas it is preferable to map requirements in the URM to external requirements, as depicted above, it should generally not be the case that an organization starts with the external requirements, but rather starts with the business requirements and then maps the external requirements into the ERM, adding or modifying requirements as necessary when gaps are identified between the URM and external requirements.

One thing to take into consideration when defining requirements is the flow of the requirements throughout the organization. . Consider the flow of requirements depicted in Figure 3 below:

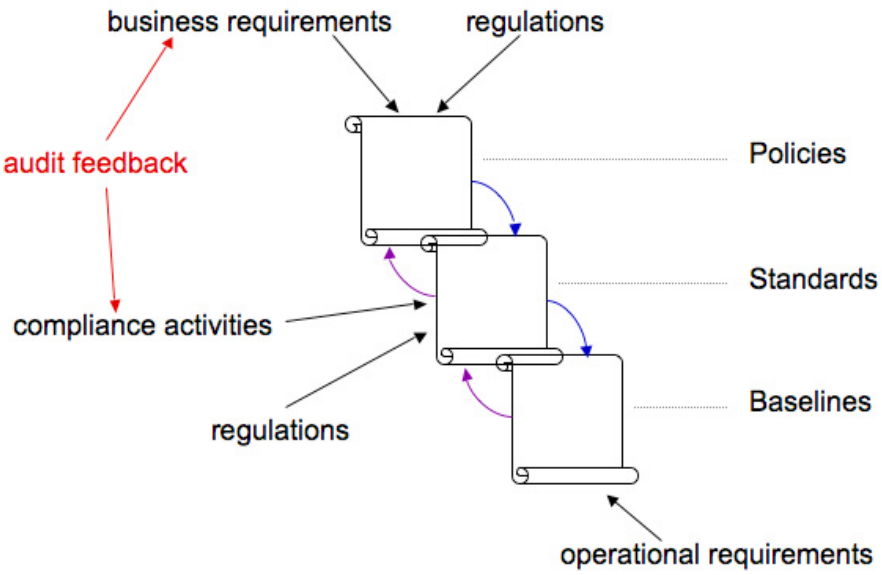

Figure 3: Flow of Requirements

Specifically, it is important to ensure that requirements not only flow down from the strategic to tactical to operational levels of the organization, but that feedback flows back up to the top. For example, if there are operational constraints with a given technology that would prohibit reasonable implementation of a given requirement, then those constraints need to be communicated up the chain of command and the requirement should be amended and documented accordingly. Also, as demonstrated within the model by the lifecycle approach, the URM is not a "write once, implement once" component, but is a living description of requirements that must be continually updated and refined to meet the needs of the business and external regulations.

Mapping the policy framework to the URM, as well as how it fits within the overall model, is discussed below.

> ***Example:*** With the Payment Card Industry Data Security Standard (PCI DSS), it is required that the full credit card number be encrypted in storage. At the business level, it might seem like a logical step to simply declare that the entire database containing full credit card numbers be encrypted. However, one should also consider this stance from an operational standpoint; particularly from the view of performance. While encrypting all data in a given database might be convenient in the policy realm, it may well be found that the overall load of these cryptographic operations results in additional hardware requirements, as well as an overall reduction in application performance. By including operations personnel in the policy evaluation process, with specific methods for providing feedback up the chain of command, you can minimize some of these collisions between desired policy stance and realistic ability to implement the policy.

Resolving Conflicting Requirements

Inevitably, requirements are going to conflict with reality or other requirements. In a situation where a conflict arises, mediation should occur between all three competencies. This mediation should occur jointly and civilly, bearing in mind that ultimately the business (represented by ERM delegates) must accept the risk associated with the trade-off to be made between requirements.

The following general approach may be useful in resolving conflicts:

1. Identify the conflict.
2. Confirm that the conflict exists – is it a simple conflict that may be resolved by choosing the most secure option, or is it a fundamental conflict that will require a trade-off?
3. Identify the source of each requirement and any penalties associated with choosing not to meet each (including business cost, fines, etc.).

4. Determine if the requirements can be fulfilled adequately through compensating controls that may not conflict. For example, physical segregation of environments may be too expensive, but logical segregation may be achieved at a more reasonable cost through alternative controls (virtual machines, role-based access controls, etc.).
5. Determine if the scope of each requirement can be limited to see if the conflict can be reduced or eliminated.
6. Weigh all options. Ensure that each option is feasible. Ensure that the cost of failed compliance, if applicable, is included.
7. Make the hard trade-off decision. Ultimately, this is the role of the business (ERM).
8. Document the exception within the Universal Requirements Matrix (URM). **NOTE: It is imperative to thoroughly document exceptions in order to provide evidence to auditors of due diligence being performed.

In addition to URM conflicts, there may also be conflicts resulting from enterprise re-organization activities, including situations resulting from mergers and acquisitions. The TEAM model represents a generic approach that should be resilient to organizational change.

Notwithstanding, if one organization has adopted the TEAM model and the other has not, a case will need to be made for adoption. One key argument could be that adoption of the TEAM model should be straightforward and painless, while hashing out preferred methods within each competency may be more challenging. At the same time, by assigning conflicting organizational components into each competency, mediation should be more efficient and effective because competing organizational components will be on an even footing, allowing for

apples-to-apples comparisons, and possible development of a hybrid approach synergizing "competing" visions.

In the end, all parties must be prepared to accept that the optimal solution may not be achieved. Consider the following three examples.

Example 1: *Sometimes, legacy wins*. No matter what regulations may required for compliance, there will be cases where legacy systems and applications simply cannot be brought into conformance. For example, mainframe technologies are trailing behind mainstream system evolution in key areas such as network security. Regulations may require that remote administration of systems in-scope be performed over a secure network connection. However, many mainframe solutions today still employ a TELNET-based communication protocol for remote access (TN3270 uses TELNET). TELNET does not encrypt communications in-transit, and mainframe TELNET services may not support integration with secured authentication packages like Kerberos (which would at lease prevent credentials from crossing the network unencrypted). In cases like these, where legacy technology either does not have options available for compliance, or where the cost of conforming may significantly outweigh the cost of the penalties for not confirming, the business will necessarily have to choose to document the system as an exception, with an adequate explanation provided to auditors.

One note to attach to this example is that there may be suitable alternatives with compensating controls. For example, instead of allowing direct TELNET access to mainframes, one could instead use network-based controls to limit access only from approved hosts. Taking this idea one step further, jump hosts (also known as bastion hosts) could be setup that support secure remote access (such as via SSH) from approved personnel. Access into the legacy systems could then be limited to only these secured hosts. Access to the secured hosts could be logged, in accordance with regulations. If these jump hosts were placed within close network proximity to the legacy systems, then the exposure of unencrypted network traffic would be limited significantly.

Example 2: *Sometimes, regulations win*. There may be situations wherein compliance with regulations is not optional. For example, federal agencies often do not have the option of choosing between what regulations they will and will not comply with. In these situations, efforts such as budgetary processes will need to be leveraged to plan accordingly for the additional expenses that may be incurred. If additional funding cannot be identified to perform necessary compliance activities, then the funding may need to be taken from other projects of lower priority that may be accomplishing non-regulatory objectives, such as improving efficiency or effectiveness. These types of funding redirections should be highlighted for auditors (or the Inspector General) to underscore the true cost of compliance. However, rational minds will likely point out that pointing out the deficiency will likely not have any impact on future funding or even positively influence associated reports. Learning to do more with less seems to be the mantra of modern enterprises.

Example 3: *Sometimes, nobody wins*. Organizations should be prepared for the worst-case scenario wherein significant amount of money are dedicated to compliance efforts, only to fail in the end, either due to a misunderstanding of requirements, or because the nature of the requirements may have shifted during remediation activities. Example 2 above describes a situation where efforts to be compliant with requirements may cause redirection of funding from other important projects due to limited funding. Imagine this scenario resulting in a system that is not in the end compliant with the requirements specified.

Enterprise Risk Management (ERM)

The Enterprise Risk Management competency area represents the role of business management within the overall Assurance Management approach. Ultimately, ERM owns the URM, representing the interests of the business and setting the strategic approach for the enterprise. How the organization implements ERM is at the discretion of the organization. There is no "one size fits all" approach that is best suited to all organizations, regardless of purpose and function.

Instead, the ERM should be approached from a combined perspective of seeking out best practices, while ensuring that the competency area is implemented according to a lifecycle that facilitates continuous quality improvement. In some cases, it may be useful to implement a framework such as the "Enterprise Risk Management – Integrated Framework" by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In other cases, it may be best to develop a custom framework that incorporates other best practice approaches, such as the Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) methodology, or the McCumber Cube for risk modeling.

The key take-away points for the Enterprise Risk Management competency are as follows:

- Focuses on business requirements using a risk management approach
- Should use iterative lifecycle approach
- Adopts industry best practices, as appropriate
- Effectively "owns" the Universal Requirements Matrix
- Sets strategic direction for Assurance Management program
- Determines framework(s) and methodologies for assessing and managing risk
- Communicates direction to the Operational Security Management competency
- Receives feedback from the Audit Management competency area

Operational Security Management (OSM)

Whereas the ERM phase defines and communicates requirements, stipulating the criteria by which risk is to be managed, it is the responsibility of the Operational Security Management competency to implement those requirements, providing direct feedback on the operational impact of directives, including cases where conformance is not feasible. In short, where ERM "plans," OSM "does."

Within the OSM, an iterative lifecycle approach should be used that incorporates best practices that pertain to the implementation of security countermeasures and controls. Frameworks like ISO/IEC 17799/27001 or the Information Security Management Maturity Model (ISM3) may be worth implementing to support this overall effort. Furthermore, other targeted frameworks and methodologies may be useful, such as the InfoSec Assurance

Capability Maturity Model (IA-CMM) and its associated methodologies for performing attestation within the operational organization.

The focus of OSM is in supporting the enterprise. While this phase may be thought of as synonymous with IT security activities, such as access management, it could also include other security areas, such as physical security.

The key take-away points for the Operational Security Management competency are as follows:

- Should use iterative lifecycle approach
- Adopts industry best practices, as appropriate
- Implements the Universal Requirements Matrix
- Aligns with the strategic direction of the Assurance Management program, as set by the Enterprise Risk management competency
- Determines framework(s) and methodologies that best meet the requirements of the URM while optimizing operations
- Identifies URM requirements that are not feasible or are in conflict and initiates the conflict resolution processes
- Assists the Audit Management competency area in providing documentation and access to systems and applications in support of audit activities

Parallels Between Policies and URM, ERM, and OSM

Before moving on to discuss the role of Audit Management within the TEAM model, it is first instructive to take a sidebar into the topic of policies. When considering the role of the Universal Requirements Matrix, it is a logical progression to link it to the policy framework of

the organization; specifically, the security policies that must be defined in accordance with various regulations (e.g., Sarbanes-Oxley, PCI DSS).

The traditional policy framework generally follows the hierarchical structure of organizations. A small number of top-level policies equate to the strategic (or executive) level of the organization. These policies set the direction for security practices across the enterprise and feed into more detailed documents at the tactical level, often called standards. Below standards, feeding into the operational level of the organization, are more detailed, specific documents such as procedures, guidelines, and baselines. Shown graphically, a policy framework may look as depicted in Figure 4 (next page).

Considering the mapping of policies, standards, and baselines to the organizational levels of strategic, tactical, and operational, it is then logical to desire mapping these constructs into the ERM and OSM competency areas, as well as into the overall TEAM model. Figure 5 below shows how the policy framework depicted in Figure 4 overlays onto the TEAM model.

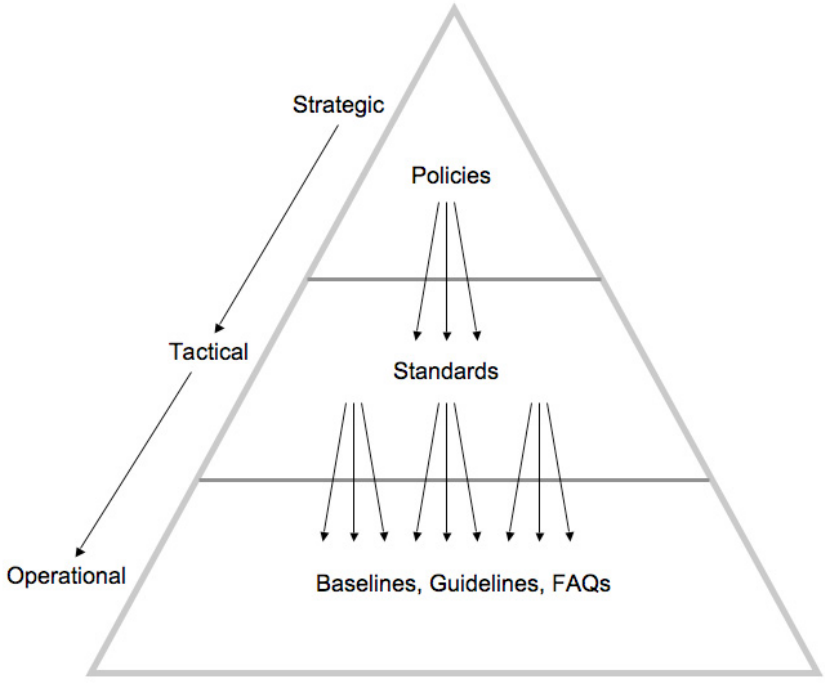

Figure 4: Generic Policy Framework

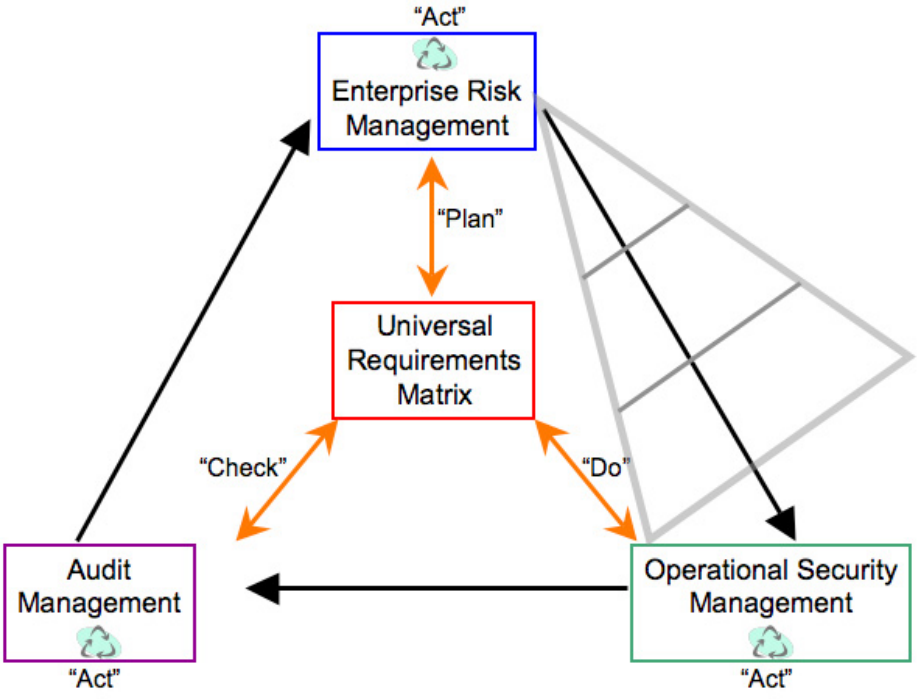

Figure 5: Policy Framework Overlaid

The policy framework is ultimately owned by the business, which is represented by the Enterprise Risk Management competency area. As such, the top-level policies must be set by the ERM as a vehicle for communicating direction and strategy to operations. At the base of the policy framework reside the detailed baselines and procedures that apply directly to operational personnel charged with implementing the strategy set by the business.

In the mid-tier of the policy framework rests a transitional zone that maps very well to the transition point in the TEAM model between ERM and OSM. This section of the policy framework should be jointly owned by the business and operations, providing a sort of glue between the high-level policies written in business, risk management terms and the baselines written in operational terms that can be directly implemented.

Notably absent from the policy framework is the influence of the Audit Management competency. This will be discussed further below. In brief, the audit function may play a peripheral role in the policy framework, as in the case of the Universal Requirements Matrix, but auditors must not cross the line into writing or dictating policies, standards, etc. This requirement may appear to put the organization at a disadvantage, ignoring the expertise of a competency area that may have good, legitimate ideas to contribute. However, it is vital to remember that the audit function must maintain a degree of independence from the rest of the organization.

Audit Management (AuM)

The Audit Management competency area represents the linchpin in the check-and-balance approach leveraged by the TEAM model. The role of the AuM competency is to audit (or "check") for organizational compliance with the URM, as well as perform gap analysis

between the URM and external regulations from legislation and industry. Any deficiencies should then be reported into the ERM phase to continue the lifecycle.

As with the other competency areas, the AuM should be based on an iterative lifecycle approach. Best practices, such as COBIT, can be leveraged in structuring this phase of the model. Analogously, this function may be thought of as being similar to the judicial branch of the US federal government, providing a counterbalance to the two other key areas.

The key take-away points for the Audit Management competency are as follows:

- Should use iterative lifecycle approach
- Adopts industry best practices, as appropriate
- Checks the implementation of the Universal Requirements Matrix
- Works hand-in-hand with the Operational Security Management competency area in getting access to documentation, systems, and applications in support of the audit function
- Reports findings to the Enterprise Risk Management competency area
- Maintains a high degree of independence from the ERM and OSM competencies so as to remain objective, including independence in the chain of command

Tips for Implementing the TEAM Model

At face value, implementation of the TEAM model may seem like a daunting task that entails massive reorganization, generation of reams of new documentation, and millions of dollars in overhead expenditure. However, if done smartly, this should not be the case.

Tip #1: Leverage Existing Structures

Chances are good that most organizations have many of the key pieces that go into ERM, OSM, and AuM. For example, an existing internal audit team is a natural fit for AuM, even if IT audit responsibilities are not currently handled by the team. Similarly, if there are dedicated security resources within the operations ranks, then it is logical to leverage those resources within the OSM. ERM may be the most challenging competency area to organize given the challenges in finding people with strong skill sets in both business management and technical risk analysis.

Tip #2: Use a Phased Approach

It might be tempting to make whole-scale changed within an organization to quickly adapt the TEAM model. However, given some time to analyze the changes necessary, eagerness may quickly turn to fear, depression, or loathing. Instead of tackling the entire problem, it is highly recommended that a phased approach be used. Remember the KISS principal: Keep it Simple, Silly.

Tip #3: Perform Tasks in Parallel

In slight contrast to Tip #2, it is also recommended that certain tasks be performed in parallel. For example, collecting or creating documentation of existing practices can be performed alongside overall planning for organizational restructuring. Branching activities like this can help keep all stakeholders engaged, whereas leaving lots of downtime can result in straying attention spans.

Tip #4: Avoid Leadership by Committee

Ultimately, it is of vital importance that one person be responsible for overall implementation of the TEAM model. That leadership role descends naturally from the

responsibilities of the ERM competency. This is not to say that a central committee should not be formed to drive this initiative. Quite the contrary, it is of the utmost importance that all key stakeholders be involved equally. Nonetheless, the likelihood of project floundering is higher without a single clear leader to keep the project on-target.

Tip #5: Be Flexible

This model is provided as a general guideline for structuring a full-scale enterprise assurance management approach. However, given that it is a theoretical model, it is subject to the pitfalls associated with real life. If something described here doesn't work for a given organization, then change it. Similarly, if something isn't working within your organization, then change it. Do not unnecessarily bind present and future decisions to previous decisions that may no longer be correct or accurate.

The Importance of Independence

It is important to take a sidebar at this point to underscore the importance of establishing and maintaining independence between the Audit Management competency area and the Enterprise Risk Management and Operational Security Management competencies. Given that the role of the auditor is to perform audit tasks that check for compliance with requirements (such as those detailed in the Universal Requirements Matrix) and with applicable regulations, it is particularly important that the auditor not then be checking their own work. Thus, by definition, the AuM area must maintain independence, only reporting on discrepancies to the ERM area, allowing the ERM area to take corrective steps to influence the OSM area to comply. In short, independence correlates to objectivity and increased effectiveness of the audit function.

Not only is independence important for the maintenance of objectivity, but it is also a legal requirement, enforced in the United States via the Independence Standards Board in the late 1990s and presently by the Public Company Accounting Oversight Board (PCAOB). The U.S. Securities and Exchange Commission has established the authority of the PCAOB. More information about independence can be found at the following web sites:

- Final Rule: Strengthening *(sic)* the Commission's Requirements Regarding Auditor Independence – http://www.sec.gov/rules/final/33-8183.htm
- ET Section 100 INDEPENDENCE, INTEGRITY, AND OBJECTIVITY – http://www.pcaobus.org/Standards/Interim_Standards/Ethics/et_100.html

The Complete TEAM Model

Combining the basic TEAM model with the policy framework overlay depicted in Figure 4 and the necessity for independence results in the final, complete depiction of the TEAM model in Figure 6 below.

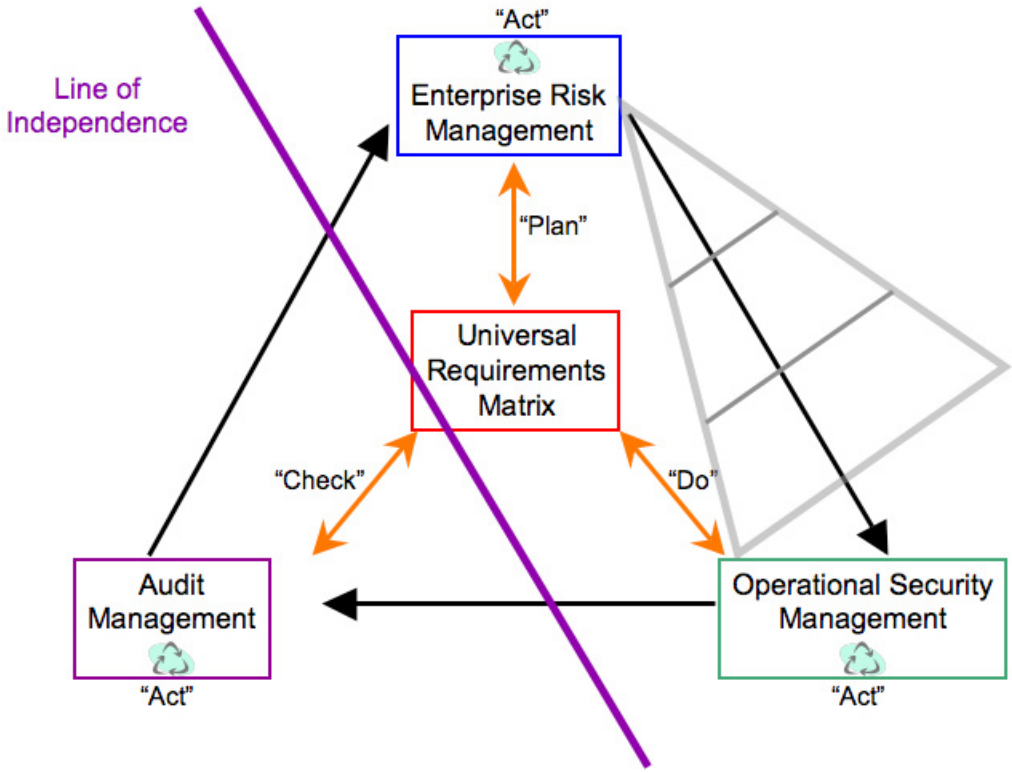

Figure 6: Complete TEAM Model

It is worth noting that the line of independence does not completely remove the Audit Management phase from having interaction with the URM. The AuM is responsible for reviewing the URM to ensure that gaps do not exist between the requirements it contains and those levied upon the organization from external entities.

Suggested Management Structure

In keeping with the requirement for independence, the suggested management structure surrounding the TEAM model may look like the following:

- ERM: CEO, CIO, COO

- OSM: CTO, CISO, CIO, COO
- AuM: CFO, VP of Finance, Internal Audit Committee

It is possible that the same executive may head the ERM and OSM competencies, but it is again imperative that the AuM competency report to a separate executive in order to maintain independence.

Scalability of the TEAM Model

The subject of scalability with respect to the TEAM model is one that cannot be answered definitively without the support of test implementations. However, it is the intent that this model be flexible enough to support organizations of all size, with or without modification.

Ultimately, it's worth noting that this model could be implemented in an organization with as few as two people. The magic number of two derives from the need to establish and maintain independence between ERP/OSM and AuM. However, this model can also realistically be implemented in larger organizations.

The reason that large organizations can use the TEAM model stems from the high-level focus on the key competency areas, rather than focusing on specific practices or technologies. Because of this general focus, organizations should be able to concentrate resources within each competency, allowing each area to grow to meet the needs of the business, and be concerned mainly with establishing and maintaining the overall flow and containment of responsibilities.

As is the nature of large organizations, it may at first seem to be an uphill battle trying to group personnel by competency area. For example, multiple groups might be performing attestation activities that may seem to fit under and or all of ERM, OSM, or AuM. However, an

analysis of actual activities being performed may result in clarification of a seemingly muddy picture.

There are likely numerous cases where categorization of activities into one of the three competency areas may seem daunting. However, once these activities are properly labeled and attached to a competency, it should hopefully become easier to integrate those activities within the competency.

Positive side effects of going through the process of analyzing resources with similar responsibilities should be an improvement in efficiency and effectiveness. Additionally, analysis may uncover unnecessarily duplicated efforts that can be merged and consolidated. As part of the consolidation, the opportunity may then present itself to cherry-pick practices that are best suited to the organization, also potentially resulting in improved efficiency and effectiveness.

Compliance: Everyone's Job

One topic that has not been discussed in this document is the place for compliance. The act of being compliant has been mentioned in specific relation to the AuM function testing the organization and the URM. However, it is worth noting that compliance (along with conformance) is not an activity limited to the audit function. In fact, compliance is the responsibility of everyone in the organization. To be compliant, however, implies that requirements are effectively communicated to everyone within the organization. Enter the role of the policy framework, among other tools for communication, such as education, training and awareness programs.

V. Findings and Conclusions

The research process was divided into three phases. Phase 1 involved the collection and documentation of information assurance methods. Phase 2 created an overarching model for assurance management that harmonized the key competency areas of enterprise risk management, operational security management, and audit management around a central axis of defined requirements. Phase 3 validated this approach through the targeted solicitation of feedback from subject matter experts.

To recapitulate, the following diagram describes the model created in phase 2:

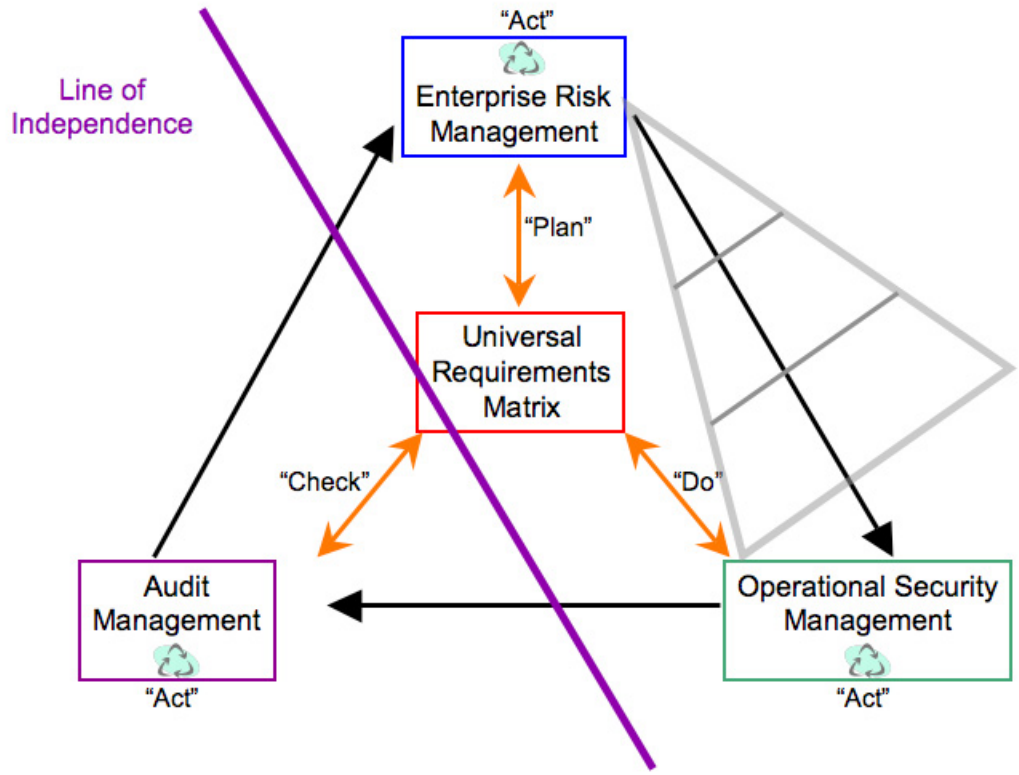

Figure 7: Recap - The Complete TEAM Model

The model is comprised of four key components: the Universal Requirements Matrix and the three key competencies (Enterprise Risk Management, Operational Security Management, and Audit Management). The three competencies are arrayed around the URM in a lifecycle approach that follows the ISO Plan-Do-Check-Act methodology. However, rather than establishing a single Act phase, the Act phase is distributed across all three competencies, which in turn are charged with implementing a lifecycle for its own responsibilities, preferably based on best practices.

In addition to the four key components, the model incorporates an overlay of the typical policy framework, which starts at the strategic level of an organization at the ERM competency area, and descends transitionally to the operational level of an organization, terminating in the OSM competency.

Finally, the AuM competency is segregated from the other two competencies by a line of independence, required by law and to maintain objectivity. Furthermore, the line delineates the suggested separation in management structure between AuM and the other areas.

Subject Matter Expert (SME) Feedback: Descriptive Analysis

Of the twenty-four (24) subject matter experts (SMEs) invited to participate in Phase 3 of the thesis research, one (1) opted out of participating altogether, one (1) opted out of the formal survey, and eleven (11) participated in the survey, for an uptake rate of just over 45%. In general, all questions answered, except one (#12), leaned in a positive direction of support for the research. In addition to the survey response, several participants also provided extended comments via email and/or phone.

The survey was delivered online via Zoomerang.com. Each SME was emailed a unique URL for participation at survey commencement on 17 March 2006. Reminders were sent on 23 March 2006 and 28 March 2006 to those who had not yet responded. The survey was closed on 2 April 2006. The full text of the survey can be found in Appendix A, and the full survey results are provided in Appendix B. Statistics listed within this analysis may only add up to 99% as a result of rounding errors.

Based on direct and survey feedback, the following topics were reviewed and bolstered within Section IV above:

- Description of the URM was updated to better denote business requirements coming first, with external requirements mapping into business requirements, not the other way around.
- Reference to PDCA in the Model Overview was clarified to explain intent and decisions made.
- A more lengthy discourse was provided on the topic of scalability.
- A section was added discussing resolving requirement conflicts.
- Wording was added to reinforce that the TEAM model is ultimately a risk-driven approach.

Following are some general highlights of the survey pertain to overall impression of the research:

- 73% viewed the work favorably
- 91% agreed that the TEAM model is a logical approach to assurance management
- 73% agreed with the conclusions of the research
- 73% agreed that the TEAM model is feasibly implemented

- Only 46% thought it likely that they would implement the TEAM model when given the opportunity
- On average, SMEs spent approximately 5 hours reviewing the research, with a low of 2 hours and a high of 10 hours.

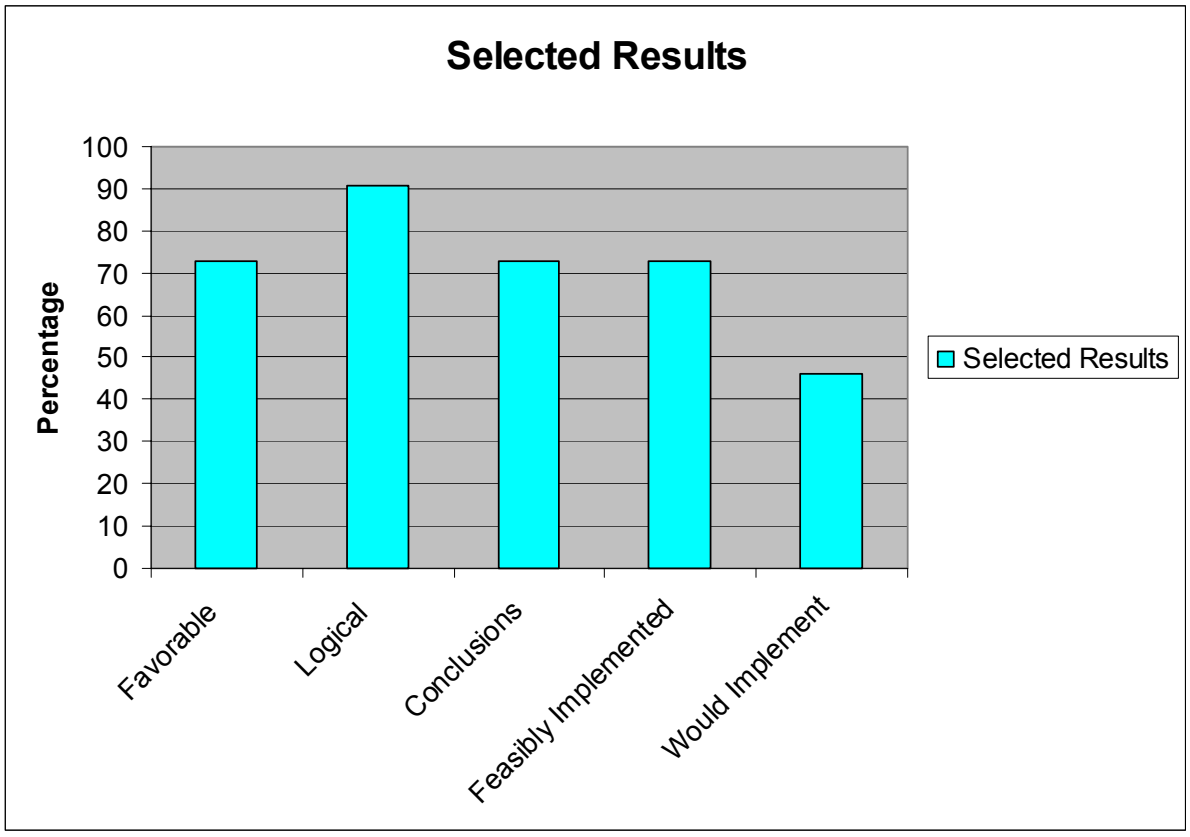

Figure 8: Selected Results

The survey also sought to quantify the general bias of the SMEs about the three (3) competency areas and the four (4) objectives stated in the hypotheses. When asked to rank, from most to least important, respondents turned in the following results for competencies:

1. Enterprise Risk Management (64%)
2. Operational Security Management (64%)
3. Audit Management (91%)

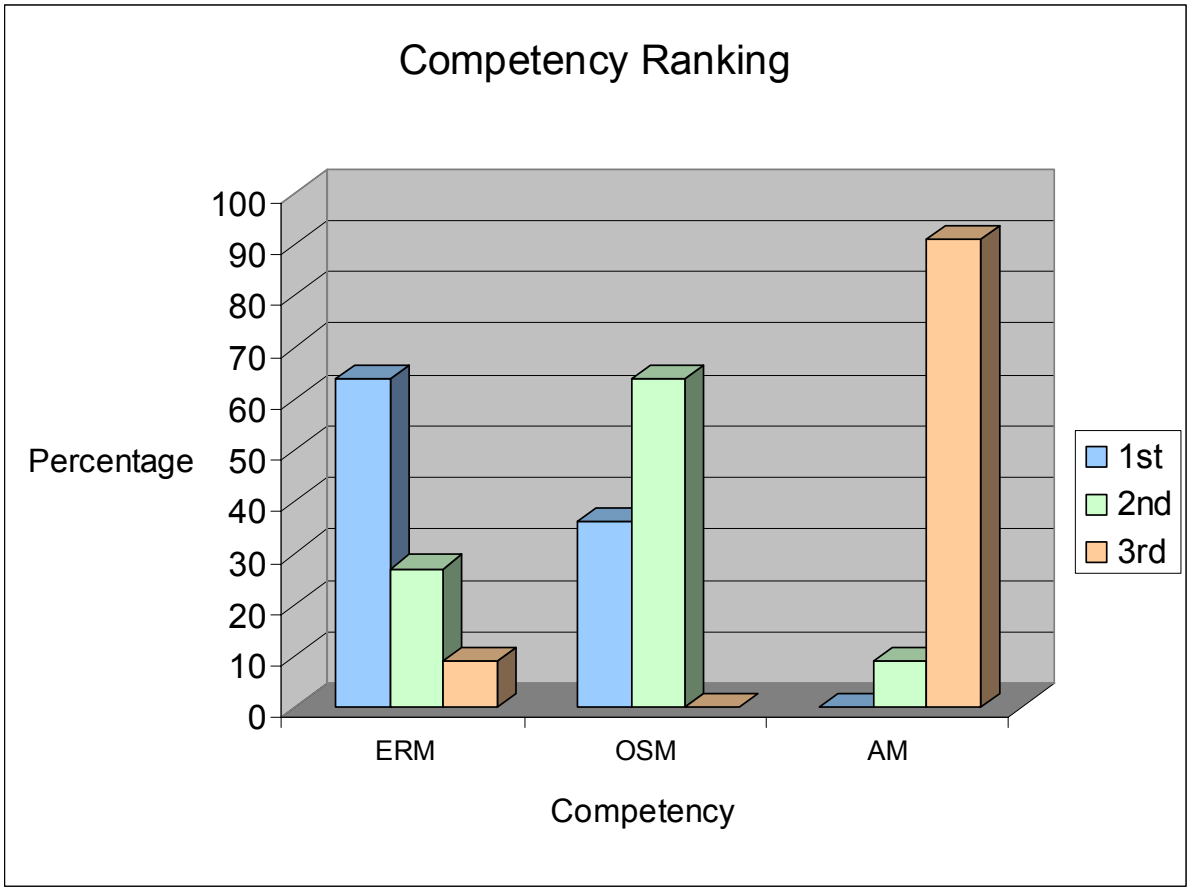

Figure 9: Ranking of Competencies

Figure 9 above shows the overall ranking results for the competencies. The ranking results are quite clear when depicted this way. An alternative way of looking at the results is depicted in Figure 10 below. A power ranking approach was used to create a single combined result for each competency. The power ranking multiplies the number of votes in a given place (1st, 2nd, or 3rd) for each competency by a corresponding numerical value (in this case, 9 points for 1st, 6 points for 2nd, and 3 points for 3rd). The points were then added across for each competency to see if the overall score correlated to the individual ranking results. In this case, the results are consistent, with ERM being 1st, OSM 2nd, and AM 3rd.

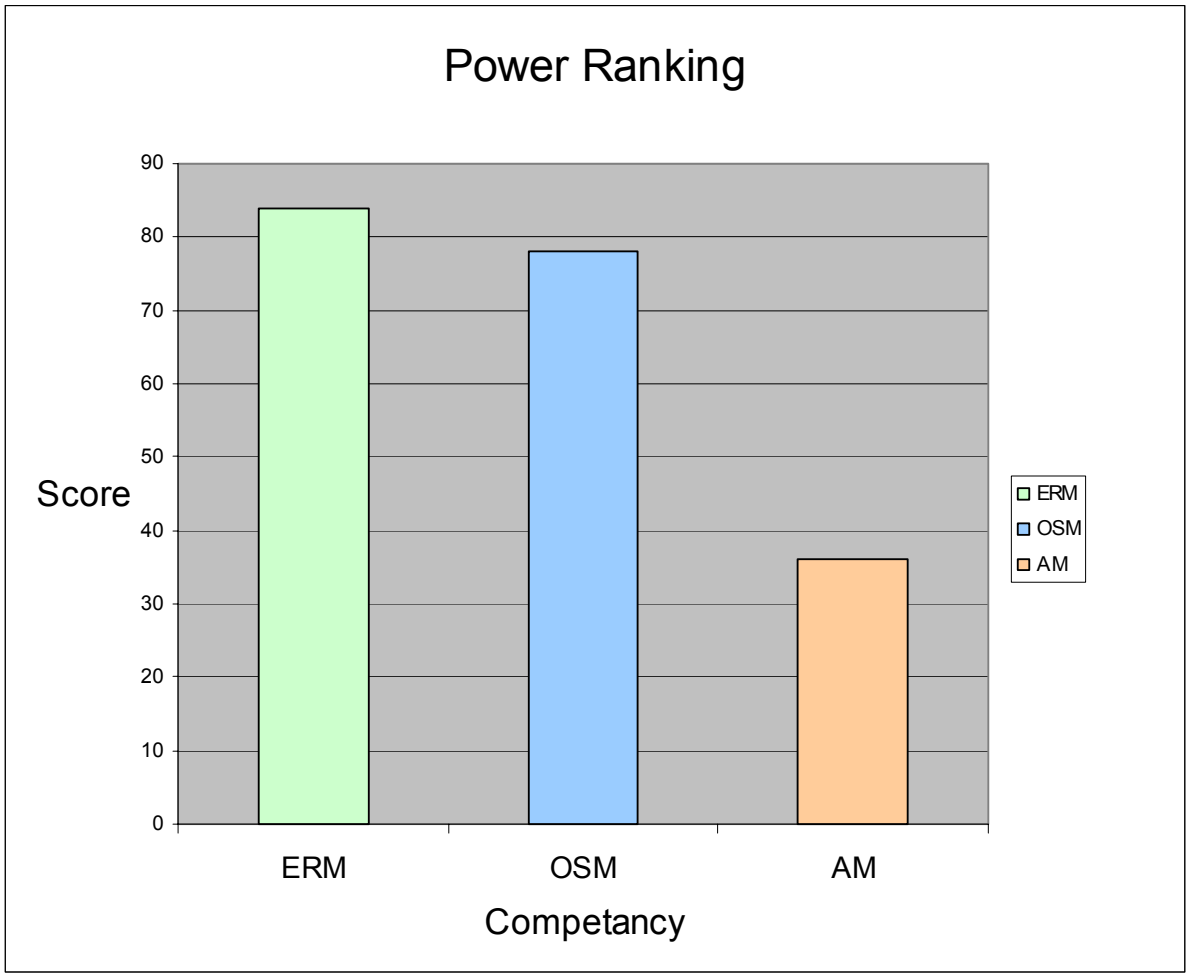

Figure 10: Power Ranking of Competencies

For ranking the hypotheses, respondent rankings produced the following results:

1. Better Management of Risk (55%)
2. Effectiveness (36%)
3. Efficiency (45%)
4. Optimized Operations (45%)

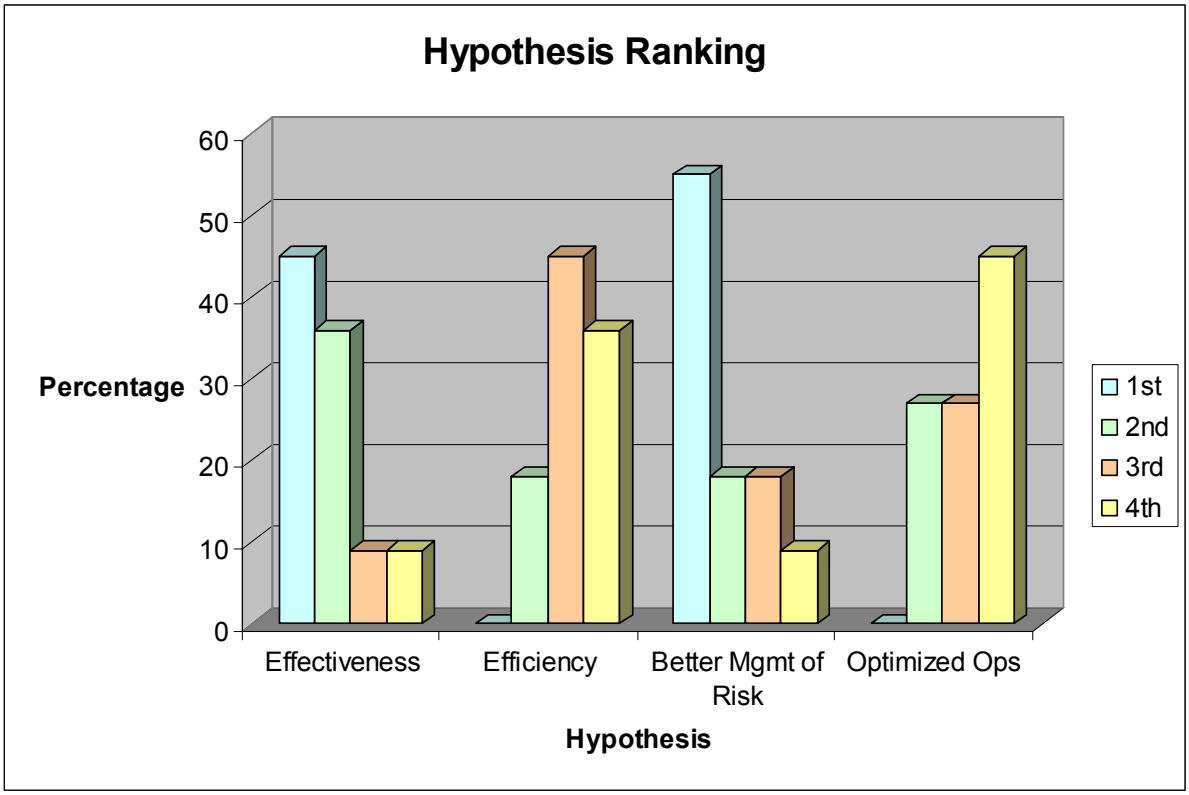

Figure 11: Hypothesis Ranking

Figure 11 above shows clearly that Better Management of Risk received the most votes as ranking 1st, though Effectiveness was not far behind, eventually ending up as ranked as 2nd most important. Efficiency was distinctly rated as 3rd most important, and Optimized Operations was significantly ranked as least important of the four hypotheses.

Figure 12 below shows power ranking results of the voting, showing a lack of parity in the rankings on an individual basis. What is clear from the power ranking is that Better Management of Risk and Effectiveness are clearly placed as the top two priorities, whereas Efficiency and Optimized Operations are definitively ranked as the lowest priorities.

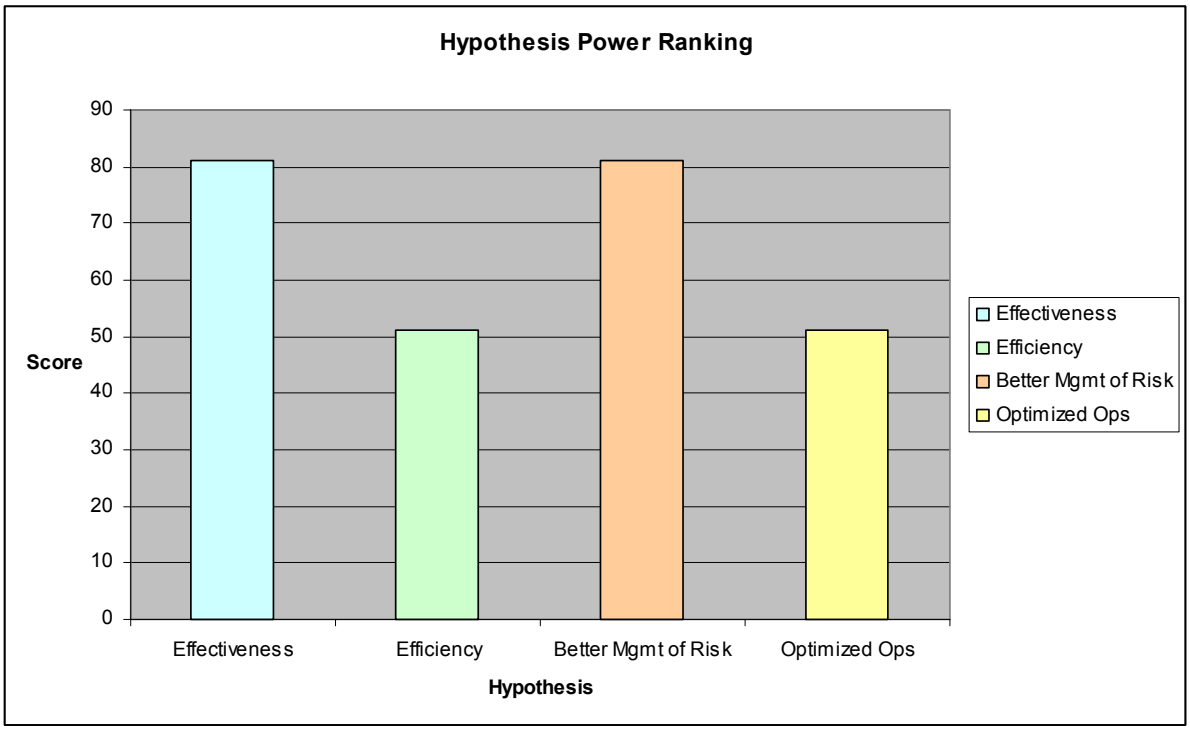

Figure 12: Power Ranking of Hypotheses

As can be seen within the full results in Appendix B, there was a high degree of consensus on the first ranking exercise. However, the second ranking exercise had a slightly more diffuse result, with the second choice being particularly contentious. In addition to the 36% ranking of Effectiveness in 2nd, 27% ranked Optimized Operations at this level, with 18% ranking each of Efficiency and Better Management of Risk at this position. Interestingly, while positions two through four were somewhat disputed, the first position was split 55:45 between Better Management of Risk and Effectiveness.

Given these preferences, the respondents then were asked questions designed to specifically validate the thesis hypotheses. The following results are listed by hypothesis with the corresponding results from the internally consistent and validating questions:

- H1a: Organizations that adopt a unified approach to information assurance will be more efficient than organizations that do not adopt a unified approach.

    - 73% agreed that the TEAM model encourages efficient assurance management.
    - 64% agreed that organizations adopting the TEAM model would be more efficient than those that do not adopt a unified approach.
- H1b: Organizations that adopt a unified approach to information assurance will be more effective than organizations that do not adopt a unified approach.
    - 63% agreed that the TEAM model encourages more effective assurance management.
    - 82% agreed that organizations adopting TEAM model would be more effective than those that do not adopt a unified approach.
- H1c: Organizations that adopt a unified approach to information assurance will manage risk better than organizations that do not adopt a unified approach.
    - 55% agreed that the TEAM model encourages better risk management.
    - 73% agreed that organizations adopting the TEAM model would manage risk better than those that do not adopt a unified approach.
- H1d: Organizations that adopt a unified approach to information assurance will optimize their operations better than organizations that do not adopt a unified approach.
    - 55% agreed that the TEAM model encourages optimized operations.
    - 54% agreed that organizations adopting the TEAM model would optimize operations better than those that do not adopt a unified approach.

The following graph shows the scores above, by hypothesis, with green representing the "encourages" questions and the blue representing the "adoption" questions described above.

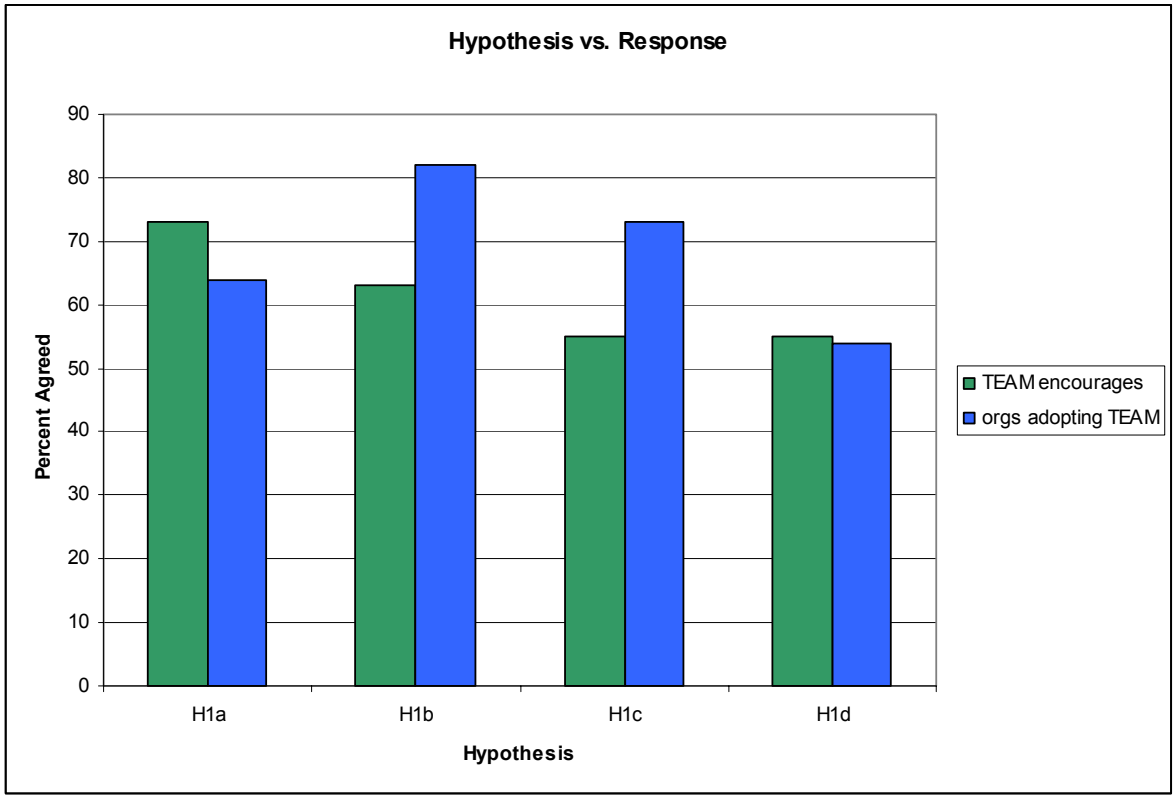

Figure 13: Hypothesis vs. Response

Figure 13 shows that, from a purely descriptive standpoint, there is a generally positive endorsement that would indicate a trend toward achievement of the four hypotheses. However, given the lack of real implementations of the TEAM model, it is inappropriate to draw hard conclusions from the above results.

Altogether, the survey results largely validate the effort against the stated objectives. Whereas some objectives did not perform as high as might have been hoped, it is nonetheless reassuring to see all responses in the affirmative, solidly in favor of the effort.

Subject Matter Expert (SME) Feedback: Inferential Analysis

Though the survey was not constructed with an eye toward conducting inferential analysis, nor was there a clean dichotomy to draw between organizations that adopted the TEAM

model and those that did not, there were some potentially interesting results the could be derived from the research. Due to the small survey population, Fisher's exact test was used to look for relationships between paired questions. Answers of "Neutral" or "Don't Know" were excluded from the numbers used to calculate the test.

Following are selected results from this inferential analysis that demonstrate a relationship between the specified questions. A finding is significant, and thus demonstrates a relationship, if Fisher's exact test produces a result in the range of 0-5%. Full analysis results of all tests are contained in Appendix C. In total, 37 tests were executed against the data, using both a redacted and original data set. Please see Appendix C for more information. The bulleted list below indicates the summarized questions compared with the corresponding survey question number in parentheses.

- Conclusion Agreement (#11) vs. Likely to Implement (#12)

  2-tail p-value = 0.0476

- Conclusion Agreement (#11) vs. Model Feasibility (#5)

  2-tail p-value = 0.0278

- Likely to Implement (#12) vs. Model Feasibility (#5)

  2-tail p-value = 0.0476

- Likely to Implement (#12) vs. TEAM Encourages Better Risk Mgmt (#8)

  2-tail p-value = 0.0476

- Conclusion Agreement (#11) vs. TEAM Encourages Better Risk Mgmt (#8)

  2-tail p-value = 0.0357

The most striking finding of performing Fisher's exact test on the data is that many results had the 2-tail p-value = 1. It is important, however, to bear in mind that the survey was

not constructed for the performance of inferential analysis. Furthermore, because there was no test implementation of the TEAM model, the comparisons being made to test for a relationship were soft, in that they were trying to compare an unimplemented preference (such as conclusion agreement or likelihood to implement) and compare it against the more concrete hypotheses (such as that organizations would be more effective or efficient as a result of implementing the TEAM model).

With the exception of hypothesis H1c (Better Risk Mgmt), there did not appear to be any correlation between sentiments about the TEAM model and the hypotheses attempted. This conclusion contradicts the descriptive analysis above, suggesting that none or one of the hypotheses may have been proven by the research. However, these conclusions can not be made definitively given that there was not a dichotomy between implementers and non-implementers of the TEAM model.

Future Research

Whereas research must be completed in a finite period, not all work was completed as desired. The following efforts are planned as or suggested for areas of future research:

- *Alphabet Soup* white paper revisions: The current draft of the white paper looked at, among other things, now-outdated versions of COBIT, and ISO/IEC 27001, and ISM3. Since its publication, COBIT 4.0 has been released, ISO/IEC 17799:2005 has been published, and ISO/IEC 27001:2005 has been ratified and released.
    - Additional research into legislation surrounding data security and privacy would be a useful addition to this white paper.

  - Expanded research into legislation governing the organization and actions of governments, such as Clinger-Cohen and FISMA, would be a useful addition to the white paper.

- An enhanced, general population survey seeking feedback on the TEAM model may be worthwhile.
- Sponsorship of the TEAM model could be researched in order to establish it as a best practice approach.
- Integration of the TEAM model with management approaches like balanced scorecard would be useful, and would help establish the model's legitimacy.
- Identifying metrics for measuring the effectiveness, efficiency, impact on risk management, and impact on optimizing operations would help reinforce the conclusions drawn in this research.
- Implementation of the TEAM model within an organization would provide invaluable data points on the usefulness of the research to industry.

Appendix A: Full Survey Text

Following is the full text of the survey administered to the subject-matter experts via the Zoomerang.com online survey tool. This text has been derived from the web-based survey, though it has been reduced to simple text from its original format.

The following questions will be scored and are designed to establish a general baseline for the rest of the survey.

1 Please indicate your general sentiments regarding the TEAM model.
Favorable
Neutral
Unfavorable

2 Please rank the following competency areas from MOST (1) to LEAST (3) important.

1 2 3
Enterprise Risk Management

Operational Security Management

Audit Management

3 Please rank the following concepts from MOST (1) to LEAST (4) important.

1 2 3 4
Effectiveness

Efficiency

Better Management of Risk

Optimized Operations

The following questions pertain to the Total Enterprise Assurance Management (TEAM) model discussed within the Tomhave Thesis. Your answers will be cumulatively scored and your comments will be factored into pre-defense revisions.

Please indicate your level of agreement with the following statements.

4 The TEAM model is a logical approach to assurance management.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

5 The TEAM model is feasible for implementation.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

6 The TEAM model encourages more efficient assurance management.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

7 The TEAM model encourages more effective assurance management.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

8 The TEAM model encourages better management of risk.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

9 The TEAM model encourages optimized operations.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

10 The TEAM model is scalable for organizations from small to large.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

11 Do you agree with the conclusions of the TEAM model?

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

12 Given an opportunity, how likely would you be to implement the TEAM model within an organization?

Very Unlikely Unlikely Neutral Likely Very Likely Don't Know

13 Organizations that adopt the TEAM model will be more efficient than organizations that do not adopt a unified approach.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

14 Organizations that adopt the TEAM model will be more effective than organizations that do not adopt a unified approach.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

15 Organizations that adopt the TEAM model will manage risk better than organizations that do not adopt a unified approach.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

16 Organizations that adopt the TEAM model will optimize their operations better than organizations that do not adopt a unified approach.

Strongly Disagree Disagree Neutral Agree Strongly Agree Don't Know

---

The following questions are open-ended and not scored.

17 What was your overall impression of this project?

[OPEN TEXT BOX]

18 Did you find this line of research useful to industry?

[OPEN TEXT BOX]

19 Approximately how many hours did you spend reviewing this project?

[OPEN TEXT BOX]

20 (optional) Would you be willing to discuss your feedback in a 1-on-1 phone conversation?
Preferred Contact Time and Method:

[OPEN TEXT BOX]

21 (optional) Please provide your name and contact information.
Name:
Company:
Address 1:
Address 2:
City/Town:
State/Province:
Zip/Postal Code:
Country:
Email Address:

22 (optional) Would you like to receive updates regarding this work?
Preferred Contact Method:

[OPEN TEXT BOX]

Appendix B: Detailed Results of Survey

Following are the full results of the survey described in Appendix A.

Question 1: Please indicate your general sentiments regarding the TEAM model.	Question 1: Responses			
Favorable	8			
Neutral	2			
Unfavorable	1			
Question 2: Please rank the following competency areas from MOST (1) to LEAST (3) important.	Question 2: Enterprise Risk Management	Question 2: Operational Security Management	Question 2: Audit Management	
1	7	4	0	
2	3	7	1	
3	1	0	10	
Question 3: Please rank the following concepts from MOST (1) to LEAST (4) important.	Question 3: Effectiveness	Question 3: Efficiency	Question 3: Better Management of Risk	Question 3: Optimized Operations
1	5	0	6	0
2	4	2	2	3
3	1	5	2	3
4	1	4	1	5
	Question 4: The TEAM model is a logical approach to assurance management.	Question 5: The TEAM model is feasible for implementation.	Question 6: The TEAM model encourages more efficient assurance management.	Question 7: The TEAM model encourages more effective assurance management.
Strongly Disagree	0	0	0	0
Disagree	1	2	1	2
Neutral	0	1	2	2
Agree	6	7	6	4

Strongly Agree	4	1	2	3
Don't Know	0	0	0	0
	Question 8: The TEAM model encourages better management of risk.	Question 9: The TEAM model encourages optimized operations.	Question 10: The TEAM model is scalable for organizations from small to large.	Question 11: Do you agree with the conclusions of the TEAM model?
Strongly Disagree	1	0	1	0
Disagree	2	1	1	2
Neutral	2	4	0	1
Agree	2	5	8	7
Strongly Agree	4	1	1	1
Don't Know	0	0	0	0
	Question 12: Given an opportunity, how likely would you be to implement the TEAM model within an organization?			
Very Unlikely	2			
Unlikely	0			
Neutral	4			
Likely	4			
Very Likely	1			
Don't Know	0			
	Question 13: Organizations that adopt the TEAM model will be more efficient than organizations that do not adopt a unified approach.	Question 14: Organizations that adopt the TEAM model will be more effective than organizations that do not adopt a unified approach.	Question 15: Organizations that adopt the TEAM model will manage risk better than organizations that do not adopt a unified approach.	Question 16: Organizations that adopt the TEAM model will optimize their operations better than organizations that do not adopt a unified approach.
Strongly Disagree	0	0	1	0

Disagree	2	1	1	1
Neutral	2	1	1	2
Agree	6	7	6	4
Strongly Agree	1	2	2	2
Don't Know	0	0	0	2

Question 17: What was your overall impression of this project?
A needed assessment of the interraltion of these models, framworks and methodologies.
I did not find the analysis very nuanced or reflecting much insight into the various approaches mentioned.
Well researched and organized. Not withstanding that, as suggested in the Future Research section, to be most effective for organizations channlenged by this in today's marketplace, it needs to be broadened to include physical security and privacy elements.
The model is reasonable, and a quick start, very likely of help to smaller organizations with no formal risk management, but does not "unify" the various methods, models, and frameworks.
Incomplete and too advanced for practical use.
An interesting synthesis of ideas.
Very interesting reading, particularly the characterizations of the systems into models, frameworks, and methodologies. That is a very significant contribution to formalization of the way these systems are proposed and used
A very complex project, Organizations that buy into this from the top down and have very good communication infrastructure can benefit. If any breakdown it will be a people issue not a systems issue.
I think that it's a good first cut at integrating the different disciplines.
It is a nice and practical approach to managing compliance regulations in a complex environment.

Question 18: Did you find this line of research useful to industry?
Yes
I found it superficial.
Right on time for the market.
Potentially.
Yes. Exploring new ideas in methodolgies is important.
Yes. Integrated systems require integrated models that seek to reconcile competing requirements and perspectives.

Yes, the TEAM model helps to clarify the roles in information assurance and serves to define ways in which methodologies can be effectively used.
Very much so, companies and organization are always looking for ways to improvement this process. The unknown in this model is the impact of organization change when a company is acquired by another and their view on Risk is different. Then you have a clah of concepts and philosophies.
I think that it's not going to be useful to anyone for a few years. Too big a bite of the corporate silo problem at one time.
Yes, in so far as it is focused on practical application.

Question 19: Approximately how many hours did you spend reviewing this project?
4
6
5
7
2
4
6
3
10
3

Appendix C: Full Fisher's Exact Test Data

Following are the full results of the Fisher's exact test analysis performed on the data collected. Because the questions are abbreviated in the tables, the data is prefaced by a legend that defines the full question that corresponds to its short form. It should also be noted that two (2) columns of data are contrived here. The left set of data removed all answers of "Neutral" or "Don't Know." This is the true data. The right column of data does an artificial calculation based on the binary notion of "Agree vs. Does Not Agree" where "Does Not Agree" is *not* the same as "Disagree." This artificial calculation was performed for comparison purposes to determine what impact better understand of the questions might have had on the overall results.

The following list establishes the short-form and long-form of the questions represented in data:

- Conclusion Agreement: "Do you agree with the conclusions of the TEAM model?"
- Logical Approach: "The TEAM model is a logical approach to assurance management."
- Model Feasibility: "The TEAM model is feasible for implementation."
- Likely to Implement: "Given an opportunity, how likely would you be to implement the TEAM model within an organization?"
- Encour. Effective: "The TEAM model encourages more effective assurance management." (corresponds to H1a)
- Encour. Efficient: "The TEAM model encourages more efficient assurance management." (corresponds to H1b)
- Encour. Risk Mgmt: "The TEAM model encourages better management of risk." (corresponds to H1c)
- Encour. Opt. Ops.: "The TEAM model encourages optimized operations." (corresponds to H1d)

- TEAM does Effective: "Organizations that adopt the TEAM model will be more effective than organizations that do not adopt a unified approach." (corresponds to H1a)
- TEAM does Efficient: "Organizations that adopt the TEAM model will be more efficient than organizations that do not adopt a unified approach." (corresponds to H1b)
- TEAM does Risk Mgmt.: "Organizations that adopt the TEAM model will manage risk better than organizations that do not adopt a unified approach." (corresponds to H1c)
- TEAM does Opt. Ops.: "Organizations that adopt the TEAM model will optimize their operations better than organizations that do not adopt a unified approach." (corresponds to H1d)

Primary calculation of values was performed by Joseph Abramson of AOL, LLC, using Minitab. Additional calculation and verification of values was performed using a free online calculator for Fisher's Exact Test, available at http://www.matforsk.no/ola/fisher.htm.

1	Highly Insignificant
.50 - .999999	Insignificant
.25 - .50	Moderately Insignificant
.05 - .25	Borderline Significant
.0 - .05	Significant

Neutral / Don't Know Excluded		**Neutral / Don't Know Included**	
Test #1a: Conclusion Agreement vs. Logical Approach		Test #1b: Conclusion Agreement vs. Logical Approach	
B	**NB**	**B**	**NB**

A	8	0	8
NA	1	1	2
	9	1	10
			0.2

Test #2a: Conclusion Agreement vs. Model Feasibility

	B	**NB**	
A	7	0	7
NA	0	2	2
	7	2	9
			0.0277778

Test #3a: Likely to Implement vs. Logical Approach

	B	**NB**	
A	5	0	5
NA	1	1	2
	6	1	7
			0.285714

Test #4a: Likely to Implement vs. Model Feasibility

	B	**NB**	
A	5	0	5
NA	0	2	2
	5	2	7
			0.047619

Test #5a: Likely to Implement vs. Encour. Effective

	B	**NB**	
A	5	0	5
NA	0	1	1
	5	1	6
			0.166667

Test #6a: Likely to Implement vs. Encour. Efficient

	B	**NB**	
A	5	0	5
NA	0	0	0
	5	0	5
			1

Test #7a: Likely to Implement vs. Encour. Risk Mgmt

A	8	0	8
NA	2	1	3
	10	1	11
			0.272727

Test #2b: Conclusion Agreement vs. Model Feasibility

	B	**NB**	
A	7	1	8
NA	1	2	3
	8	3	11
			0.151515

Test #3b: Likely to Implement vs. Logical Approach

	B	**NB**	
A	5	0	5
NA	5	1	6
	10	1	11
			1

Test #4b: Likely to Implement vs. Model Feasibility

	B	**NB**	
A	5	0	5
NA	3	3	6
	8	3	11
			0.181818

Test #5b: Likely to Implement vs. Encour. Effective

	B	**NB**	
A	5	0	5
NA	2	4	6
	7	4	11
			0.060606

Test#6b: Likely to Implement vs. Encour. Efficient

	B	**NB**	
A	5	0	5
NA	3	3	6
	8	3	11
			0.181818

Test #7b: Likely to Implement. Vs. Encour. Risk Mgmt

	B	NB	
A	5	0	5
NA	0	2	2
	5	2	7
			0.047619

Test #8a: Likely to Implement vs. Encour. Opt. Ops.

	B	NB	
A	5	0	5
NA	1	1	2
	6	1	7
			0.285714

	B	NB	
A	5	0	5
NA	1	5	6
	6	5	11
			0.015152

Test #8a: Likely to Implement vs. Encour. Opt. Ops.

	B	NB	
A	5	0	5
NA	1	5	6
	6	5	11
			0.015152

Test #9a: Logical Approach vs. Encour. Effective

	B	NB	
A	7	1	8
NA	0	1	1
	7	2	9
			0.222222

Test #9b: Logical Approach vs. Encour. Effective

	B	NB	
A	7	3	10
NA	0	1	1
	7	4	11
			0.363636

Test #10a: Logical Approach vs. Encour. Efficiency

	B	NB	
A	8	1	9
NA	0	0	0
	8	1	9
			1

Testing #10b: Logical Approach vs. Encour. Efficiency

	B	NB	
A	8	2	10
NA	0	1	1
	8	3	11
			0.272727

Test #11a: Logical Approach vs. Encour. Risk Mgmt

	B	NB	
A	6	2	8
NA	0	1	1
	6	3	9
			0.333333

Test #11b: Logical Approach vs. Encour. Risk Mgmt

	B	NB	
A	6	4	10
NA	0	1	1
	6	5	11
			0.454545

Test #12a: Logical Approach vs. Encour. Opt. Ops.

	B	NB	
A	6	0	6
NA	0	1	1
	6	1	7
			0.142857

Test #12b: Logical Approach vs. Encour. Opt. Ops.

	B	NB	
A	6	4	10
NA	0	1	1
	6	5	11
			0.454545

Test #13a: Model Feasibility vs. Encour. Effectiveness

	B	NB	
A	6	1	7
NA	0	1	1
	6	2	8
			0.25

Test #13b: Model Feasibility vs. Encour. Effectiveness

	B	NB	
A	6	2	8
NA	1	2	3
	7	4	11
			0.490909

Test #14a: Model Feasibility vs. Encour. Efficiency

	B	NB	
A	7	1	8
NA	0	0	0
	7	1	8
			1

Test #14b: Model Feasibility vs. Encour. Efficiency

	B	NB	
A	7	1	8
NA	1	2	3
	8	3	11
			0.151515

Test #15a: Model Feasibility vs. Encour. Risk Mgmt.

	B	NB	
A	6	1	7
NA	0	2	2
	6	3	9
			0.083333

Test #15b: Model Feasibility vs. Encour. Risk Mgmt.

	B	NB	
A	6	2	8
NA	0	3	3
	6	5	11
			0.060606

Test #16a: Model Feasibility vs. Encour. Opt. Ops.

	B	NB	
A	5	0	5
NA	1	1	2
	6	1	7
			0.285714

Test #16b: Model Feasibility vs. Encour. Opt. Ops.

	B	NB	
A	5	3	8
NA	1	2	3
	6	5	11
			0.545455

Test #17a: Conclusion Agreement vs. Encour. Effective

	B	NB	
A	7	0	7
NA	0	1	1
	7	1	8
			0.125

Test #17a: Conclusion Agreement vs. Encour. Effective

	B	NB	
A	7	1	8
NA	0	3	3
	7	4	11
			0.024242

Test #18a: Conclusion Agreement vs. Encour. Efficiency

	B	NB	
A	8	0	8
NA	0	0	0

Test #18a: Conclusion Agreement vs. Encour. Efficiency

	B	NB	
A	8	0	8
NA	0	3	3

	8	0	8
			1

Test #19a: Conclusion Agreement vs. Enc. Risk Mgmt

	B	NB	
A	6	0	6
NA	0	2	2
	6	2	8
			0.035714

Test #20a: Conclusion Agreement vs. Enc. Opt. Ops.

	B	NB	
A	5	0	5
NA	1	1	2
	6	1	7
			0.285174

Test #21a: Likely Impl vs. TEAM does Effective

	B	NB	
A	5	0	5
NA	1	0	1
	6	0	6
			1

Test #22a: Likely Impl vs. TEAM does Efficiency

	B	NB	
A	4	0	4
NA	1	0	1
	5	0	5
			1

Test #23a: Likely Impl vs. TEAM does Risk Mgmt

	B	NB	
A	4	0	4
NA	1	1	2
	5	1	6
			0.333333

Test #24a: Likely Impl vs. TEAM does Opt. Ops.

	B	NB	
A	5	0	5

	8	3	11
			0.006061

Test #19a: Conclusion Agreement vs. Enc. Risk Mgmt

	B	NB	
A	6	2	8
NA	0	3	3
	6	5	11
			0.060606

Test #20a: Conclusion Agreement vs. Enc. Opt. Ops.

	B	NB	
A	5	3	8
NA	1	2	3
	6	5	11
			0.545455

Test #21b: Likely Impl vs. TEAM does Effectiveness

	B	NB	
A	5	0	5
NA	4	2	6
	9	2	11
			0.454545

Test #22b: Likely Impl vs. TEAM does Efficiency

	B	NB	
A	4	1	5
NA	3	3	6
	7	4	11
			0.545455

Test #23b: Likely Impl vs. TEAM does Risk Mgmt

	B	NB	
A	4	1	5
NA	4	2	6
	8	3	11
			1

Test #24b: Likely Impl vs. TEAM does Opt. Ops.

	B	NB	
A	5	0	5

NA	0	0	0
	5	0	5
Don't Know - 2			1

NA	3	3	6
	8	3	11
			0.181818

Test #25a: Logical Approach vs. TEAM does Effective

	B	**NB**	
A	8	1	9
NA	1	0	1
	9	1	10
			1

Test #25b: Logical Approach vs. TEAM does Effective

	B	**NB**	
A	8	2	10
NA	1	0	1
	9	2	11
			1

Test #26a: Logical Approach vs. TEAM does Efficient

	B	**NB**	
A	6	2	8
NA	1	0	1
	7	2	9
			1

Test #26b: Logical Approach vs. TEAM does Efficient

	B	**NB**	
A	6	4	10
NA	1	0	1
	7	4	11
			1

Test #27a: Logical Approach vs. TEAM does Risk Mgmt.

	B	**NB**	
A	7	2	9
NA	1	0	1
	8	2	10
			1

Test #27b: Logical Approach vs. TEAM does Risk Mgmt.

	B	**NB**	
A	7	3	10
NA	1	0	1
	8	3	11
			1

Test #28a: Logical Approach vs. TEAM does Opt. Ops.

	B	**NB**	
A	6	1	7
NA	0	0	0
	6	1	7
Don't Know - 2			1

Test #28b: Logical Approach vs. TEAM does Opt. Ops.

	B	**NB**	
A	7	3	10
NA	1	0	1
	8	3	11
			1

Test #29a: Feasible Impl vs. TEAM does Efficiency

	B	**NB**	
A	7	1	8
NA	1	0	1
	8	1	9
			1

Test #29b: Feasible Impl vs. TEAM does Efficiency

	B	**NB**	
A	7	1	8
NA	2	1	3
	9	2	11
			0.490909

Test #30a: Feasible Impl vs. TEAM does Effectiveness

Test #30b: Feasible Impl vs. TEAM does Effectiveness

	B	NB	
A	5	2	7
NA	1	0	1
	6	2	8
			1

	B	NB	
A	5	3	8
NA	2	1	3
	7	4	11
			1

Test #31a: Feasible Impl vs. TEAM does Risk Mgmt

	B	NB	
A	6	1	7
NA	1	1	2
	7	2	9
			0.416667

Test #31b: Feasible Impl vs. TEAM does Risk Mgmt

	B	NB	
A	6	2	8
NA	2	1	3
	8	3	11
			1

Test #32a: Feasible Impl vs. TEAM does Opt. Ops.

	B	NB	
A	6	1	7
NA	0	0	0
	6	1	7
Don't Know - 2			1

Test #32b: Feasible Impl vs. TEAM does Opt. Ops.

	B	NB	
A	6	2	8
NA	2	1	3
	8	3	11
Don't Know - 2			1

Test #33a: Conclusion Agreement vs does Efficiency

	B	NB	
A	8	0	8
NA	1	0	1
	9	0	9
			1

Test #33b: Conclusion Agreement vs does Efficiency

	B	NB	
A	8	0	8
NA	1	2	3
	9	2	11
			0.054546

Test #34a: Conclusion Agremeent vs does Effectiveness

	B	NB	
A	6	1	7
NA	1	0	1
	7	1	8
			1

Test #34b: Conclusion Agremeent vs does Effectiveness

	B	NB	
A	6	2	8
NA	1	2	3
	7	4	11
			0.490909

Test #35a: Conclusion Agreement vs. does Risk Mgmt

	B	NB	
A	7	0	7
NA	1	1	2
	8	1	9
			0.222222

Test #35b: Conclusion Agreement vs. does Risk Mgmt

	B	NB	
A	7	1	8
NA	1	2	3
	8	3	11
			0.151515

Test #36a: Conclusion Agreement vs. does Opt. Ops.

	B	NB	
A	6	0	6
NA	0	0	0
	6	0	6

Don't Know - 2 | 1

Test #36b: Conclusion Agreement vs. does Opt. Ops.

	B	NB	
A	7	1	8
NA	1	2	3
	8	3	11

0.151515

Test #37a: Conclusion Agreement vs. Likely to Implement

	B	NB	
A	2	0	2
NA	0	5	5
	2	5	7

Don't Know - 2 | 0.047619048

Test #37b: Conclusion Agreement vs. Likely to Implement

	B	NB	
A	3	0	3
NA	3	5	8
	6	5	11

0.181818182

Bibliography

1. Alberts, Christopher, Audrey Dorofee, James Stevens, Carol Woody. *Introduction to the OCTAVE[SM] Approach*. Pittsburgh: CME SEU, 2003, accessed 4 August 2005; available from http://www.cert.org/octave/approach_intro.pdf; Internet.

2. Alberts, Christopher J. and Audrey J. Dorofee. *Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) Criteria, Version 2.0*. Pittsburgh: CMU SEI, 2001, accessed 4 August 2005; available from http://www.cert.org/archive/pdf/01tr016.pdf; Internet.

3. Alberts, Christopher J., Audrey J Dorofee, and Julia H. Allen. *Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) Catalog of Practices, Version 2.0*. Pittsburgh: CMU SEI, 2001, accessed 4 August 2005; available from http://www.cert.org/archive/pdf/01tr020.pdf; Internet.

4. Alberts, Christopher and Audrey Dorofee. *OCTAVE[SM] Threat Profiles*. Pittsburgh: CMU SEI, 2001, accessed 4 August 2005; available from http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf; Internet.

5. Basel Committee on Banking Supervision. *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Basel: BIS Press, 2004, accessed 5 August 2005; available from http://www.bis.org/publ/bcbs107.htm; Internet.

6. Canal, Vicente Aceituno. *ISM3 1.0. Information Security Management Maturity Model*. Unknown: ISECOM, 2004, accessed 5 August 2005; available from http://isecom.securenetltd.com/ISM3.en.1.0.pdf; Internet.

7. -----. *ISM3 1.0. Quick Maturity Assessment*. Unknown: ISECOM, 2005, accessed 5 August 2005; available from http://isecom.securenetltd.com/ISM3.en.1.0.Quick_Maturity_Assesment.pdf; Internet.

8. Cangemi, Michael P. and Tommie Singleton. *Managing the Audit Function: A Corporate Audit Department Procedures Guide, 3rd Ed.* Hoboken: John Wiley & Sons, 2003.

9. Committee Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management – Integrated Framework: Executive Summary*. New York: COSO, 2004, accessed 4 August 2005; available from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf**;** Internet.

10. -----. *DRAFT: Enterprise Risk Management – Integrated Framework: Executive Summary and Framework*. New York: COSO, Undated, accessed 20 May 2004; available from (URL lost)**;** Internet.

11. Herzog, Pete. *OSSTMM 2.1. Open-Source Security Testing Methodology Manual*. Unknown: ISECOM, 2003, accessed 21 April 2004; available from http://isecom.securenetltd.com/osstmm.en.2.1.pdf; Internet.

12. -----. *OSSTMM WIRELESS 2.9.1. Wireless Security Testing Section, Open-Source Security Testing Methodology Manual*. Unknown: ISECOM, 2003, accessed 21 April 2004; available from http://isecom.securenetltd.com/osstmm.en.2.9.wireless.pdf; Internet.

13. Information Security Forum. *The Standard of Good Practice, Version 4.1*. London: ISF, 2005, accessed 24 June 2005; available from http://www.isfsecuritystandard.com/pdf/standard.pdf; Internet.

14. Information Systems Audit and Control Association. *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*. Rolling Meadows: ISACA, 2005, accessed 5 August 2005; available from http://www.isaca.org/ (membership required) as file "IS Standards Guidelines and Procedures for Auditing and Control Professionals.pdf"; Internet.

15. Institute of Internal Auditors. *Applying COSO's Enterprise Risk Management – Integrated Framework*. Altamonte Springs: IIA, accessed 4 August 2005; available from http://www.coso.org/Publications/ERM/COSO_ERM.ppt; Internet.

16. International Organization for Standardization (ISO/IEC). *ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, version 3.0 Parts 1 through 3.* Geneva: ISO, 2005, accessed 12 July 2005; available from http://www.commoncriteriaportal.org/public/expert/index.php?menu=3; Internet.

17. -----. *ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management.* Geneva: ISA, 2005.

18. -----. *ISO/IEC FDIS 27001:2005 Information technology – Security techniques – Information Security Management Systems – Requirements.* Geneva: ISA, 2005.

19. International Systems Security Engineer Association (ISSEA). *Systems Security Engineering Capability Maturity Model, Model Description Document, Version 3.0*. Herndon: ISSEA, 2003, accessed 19 April 2004; available from http://www.sse-cmm.org/docs/ssecmmv3final.pdf; Internet.

20. IT Governance Institute. *Board Briefing on IT Governance, 2nd Edition.* Rolling Meadows: ITGI, 2003, accessed 14 July 2004; available from http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf; Internet.

21. -----. *COBIT 3rd Edition Audit Guidelines*. Rolling Meadows: ITGI, 2000, accessed 14 July 2004; available as file "COBIT_Audit_Guidelines.pdf" from http://www.isaca.org/ (membership required); Internet.

22. -----. *COBIT 3rd Edition Control Objectives*. Rolling Meadows: ITGI, 2000, accessed 14 July 2004; available as file "COBIT_Control_Objectives.pdf" from http://www.isaca.org/ (membership required); Internet.

23. -----. *COBIT 3rd Edition Executive Summary*. Rolling Meadows: ITGI, 2000.

24. -----. *COBIT 3rd Edition Framework*. Rolling Meadows: ITGI, 2000.

25. -----. *COBIT 3rd Edition Implementation Tool Set*. Rolling Meadows: ITGI, 2000, accessed 14 July 2004; available as file "COBIT_Implementation_Toolset.pdf" from http://www.isaca.org/ (membership required); Internet.

26. -----. *COBIT 3rd Edition Management Guidelines*. Rolling Meadows: ITGI, 2000, accessed 14 July 2004; available as file "COBIT_Management_Guidelines.pdf" from http://www.isaca.org/ (membership required); Internet.

27. -----. *COBIT Mapping: Overview of International IT Guidance*. Rolling Meadows: ITGI, 2004, accessed 14 July 2004; available as file "COBIT_Mapping_Paper_6jan04.pdf" from http://www.isaca.org/ (membership required); Internet.

28. -----. *COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT*. Rolling Meadows: ITGI, 2004, accessed 24 June 2005; available as file "CobiT-ISO_17799-Mapping.pdf" from http://www.isaca.org/ (membership required); Internet.

29. -----. *COBIT Security Baseline: An Information Security Survival Kit*. Rolling Meadows: ITGI, 2004, accessed 24 June 2005; available as file "COBIT_Security_Baseline(web22dec04).pdf" from http://www.isaca.org/ (membership required); Internet.

30. Miles, Greg, Russ Rogers, Ed Fuller, Matthew Paul Hoagberg, and Ted Dykstra. *Security Assessment: Case Studies for Implementing the NSA IAM*. Rockland: Syngress, 2004.

31. McCumber, John. *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. Boca Raton: CRC Press, 2005.

32. Meijer, Rob J. and Rick Tucker. *State-full risk assessment & automated security incident policy environment, Version 0.3.1*. Unknown: ISECOM, 2003, accessed 21 April 2004; available from http://isecom.securenetltd.com/sipes_goal_0.3.1.pdf; Internet.

33. National Institute of Standards and Technology. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Special Publication 800-14. 1996, accessed 5 August 2005; available from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf; Internet.

34. -----. *An Introductory Resource Guide for Implementing the Healthy Insurance Portability and Accountability Act (HIPAA) Security Rule*. Special Publication 800-66. 1996, accessed 5 August 2005; available from http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf; Internet.

35. National Security Agency. *INFOSEC Assurance Capability Maturity Model (IA-CMM), Version 3.1*. Fort Meade: 2004, accessed 4 August 2005; available from http://www.iatrp.com/IA-CMMv3_1-FINAL-NOV04.doc; Internet.

36. -----. *INFOSEC Assessment Methodology: Modules 1 – 4*. Fort Meade: Undated, accessed 22 July 2004; available from http://www.iatrp.com/modules.cfm; Internet.

37. -----. *INFOSEC Evaluation Methodology: Modules 1 – 6*. Fort Meade: Undated, accessed 4 August 2005; available from http://www.iatrp.com/IEMmodules.cfm; Internet.

38. Sheard, Sarah A. and Assad Moini. "Security Engineering Awareness for Systems Engineers." *13th Annual Symposium of the International Council on Systems Engineering, Arlington, VA, June-July 2003*, accessed 1 June 2004; available from http://www.software.org//pub/externalpapers/SecEngAwareness.doc; Internet.

39. Visa U.S.A. Inc. "Payment Card Industry Data Security Standard." *Visa U.S.A., Inc., December 15, 2004,* accessed 2 November 2006; available from http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf?it=il|/business/accepting_visa/ops_risk_management/cisp.html|PCI%20Data%20Security%20Standard; Internet.

40. Taxonomy. Wikipedia.org. http://en.wikipedia.org/wiki/Taxonomy (accessed: 02 November 2006).

41. taxonomy. Dictionary.com. Dictionary.com Unabridged (v 1.0.1), Based on the Random House Unabridged Dictionary, © Random House, Inc. 2006. http://dictionary.reference.com/browse/taxonomy (accessed: 02 November 2006).

42. Model (abstract). Wikipedia.org. http://en.wikipedia.org/wiki/Model_%28abstract%29 (accessed: 02 November 2006).

43. Framework. Wikipedia.org. http://en.wikipedia.org/wiki/Framework (accessed: 02 November 2006).

44. framework. Dictionary.com. The American Heritage® Dictionary of the English Language, Fourth Edition, Houghton Mifflin Company, 2004. http://dictionary.reference.com/browse/framework (accessed: 02 November 2006).

45. Methodology. Wikipedia.org. http://en.wikipedia.org/wiki/Methodology (accessed: 02 November 2006).

46. methodology. Dictionary.com. Dictionary.com Unabridged (v 1.0.1), Based on the Random House Unabridged Dictionary, © Random House, Inc. 2006. http://dictionary.reference.com/browse/methodology (accessed: 02 November 2006).