Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies

by

Benjamin L. Tomhave

Abstract

This paper will provide a US-centric overview and analysis of commercially-oriented information security models, frameworks, and methodologies. As a necessary component of the analysis, a cursory look is taken at a sampling of applicable laws within the US, such as the Sarbanes-Oxley Act of 2002 (SOX), the Gramm-Leech-Bliley Act of 1999 (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA). Additionally, industry standards will be weighed, such as the Payment Card Industry Data Security Standard, as adopted by Visa and MasterCard. The paper will attempt to thoroughly describe the goals of these models, frameworks, and methodologies, contextualizing them within the current business, regulatory, and legislative environment, helping to identify the usefulness of each model, framework, and methodology. The analysis will demonstrate the value of each model, framework, and methodology and where application of each would benefit an organization.

Table of Contents

Table of Figures

Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies

by

Benjamin L. Tomhave

I. 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, and 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 there-after launches retaliatory strikes. In the legislative wake of these incidents arise new laws such as USA-PATRIOT and Sarbanes-Oxley. Meanwhile, States, starting with California, start discussing consumer privacy concerns and begin 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're now faced with an exponentially increasing regulatory environment, looking at the likes 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 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 in the face of greater threat of fraud and identity theft, worsened by the anonymous, mass-proliferating nature of the Internet.

To meet these growing demands, a virtual cottage industry has popped-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?

A. Overview of Approach

This paper 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, associated with the International Information Systems Security Certification Consortium ($(ISC)^2$). Section III provides a standardized listing of these methods, followed be an analysis and summary of each method's provisions. Section IV will discuss, from a US-centric standpoint, high-profile regulations (legislative and industry) and how the methods described in Section III can be leveraged against these regulations. Finally, Section V will conclude with closing thoughts.

B. Author Bias

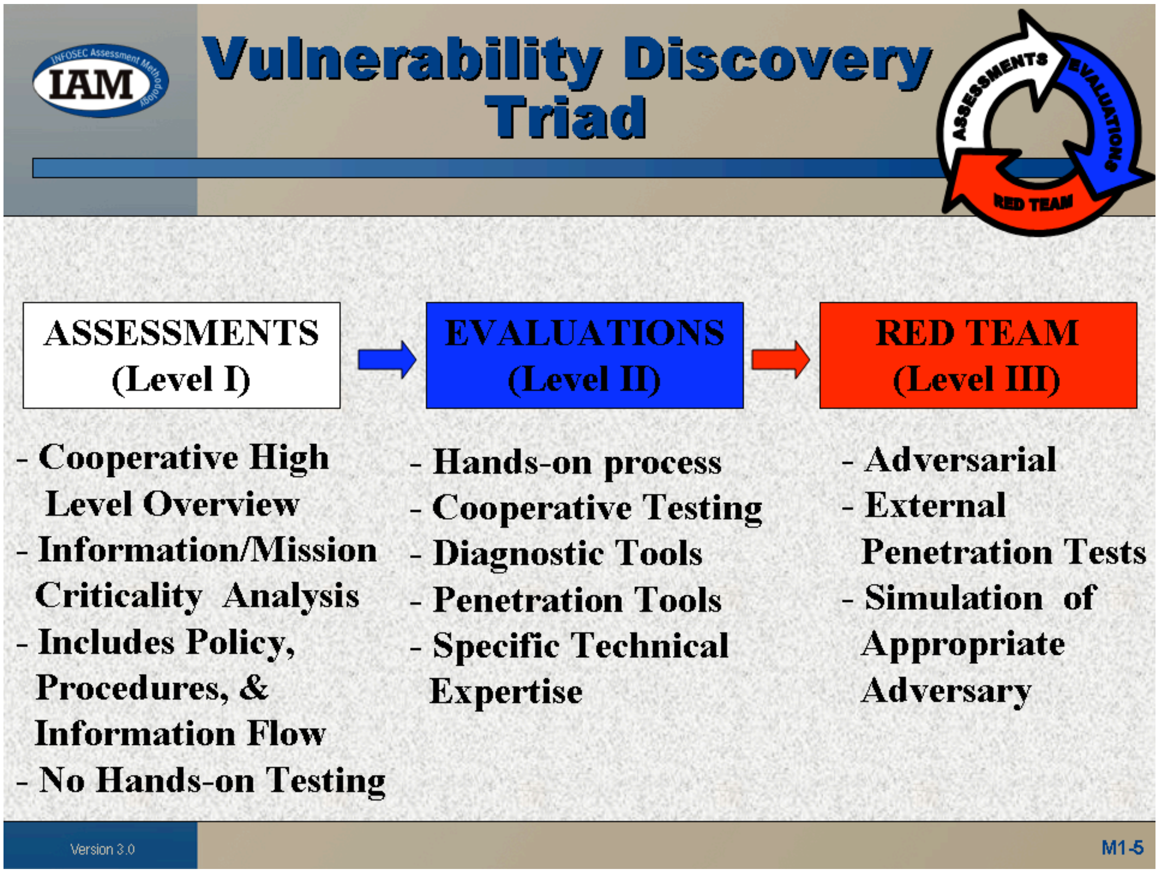
Before launching into a description and analysis of various information security methods, it is first valuable to state any biases that may affect the objectivity of the author. This author has been working within the Information Technology (IT) arena for over ten (10) years, primarily with an interest 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.

II. 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 straight-forward 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*]



Vulnerability Discovery Triad

ASSESSMENTS (Level I)

- Cooperative High Level Overview
- Information/Mission Criticality Analysis
- Includes Policy, Procedures, & Information Flow
- No Hands-on Testing

EVALUATIONS (Level II)

- Hands-on process
- Cooperative Testing
- Diagnostic Tools
- Penetration Tools
- Specific Technical Expertise

RED TEAM (Level III)

- Adversarial
- External Penetration Tests
- Simulation of Appropriate Adversary

Version 3.0

M1-5

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 the position 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[1] 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." Dictionary.com further reinforces this notion in their second definition, stating that taxonomy is "The science, laws, or principles of classification; systematics."

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.

A. 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." For the purposes of this taxonomy, a model is a high-level construct representing processes, variables, and

[1] Wikipedia can be found online at http://www.wikipedia.org/.

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.

B. Frameworks

Having defined a model as being 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 that "In software development, a framework is a defined support structure in which another software project can be organized and developed." 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."

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.

C. 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." Definition 1.a. from Dictionary.com reinforces Wikipedia, stating that methodology is "A body of practices, procedures, and rules used by those who work in a discipline or engage in an inquiry."

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

III. DETAILED OVERVIEW AND ANALYSIS

Within this section 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. A Word on Format

This section 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 speed 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.)

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.)

B. 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?

Of great significance here is noting 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 stand alone. 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 with little or no modification to 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 in III.C., 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, trying to sell this concept to senior management may be a great success or failure, 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.

C. 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 section I.B. 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 in Section IV.

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 focus 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 instead 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 in Section IV. 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 freely 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 "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

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.

D. 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^{SM}

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

Abbreviation(s): OCTAVE^{SM}, 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^{SM} (OCTAVE^{SM}) [*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 listing is provided here for completeness.

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.

IV. MEETING US-CENTRIC REGULATIONS

A common challenge facing organizations today is meeting the myriad regulations from industry and legislature. This section 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.

A. 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 in Section III 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 recap 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[2]:

1. Build and Maintain a Secure Network
   Requirement 1: Install and maintain a firewall configuration to protect data

[2] The list provided is taken from the Visa-branded PCI DSS requirements. Full information on the Visa VISP program can be found at http://www.visa.com/cisp/. Specifically, the Visa-branded draft of the PCI DSS can be located at 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.

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

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 in Section III) must be the basis for the required assessment.

B. Models, Frameworks, and Methodologies of Use

Before launching into a discourse on which models, frameworks, or methodologies may be useful in meeting the regulator 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 contingency planning.

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.

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 wish 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 do not meet the broader infosec requirements required 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 implementing 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, being that 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.

V. CONCLUSIONS AND SUMMARY

This paper 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 and SSE-CMM both hold great promise, but only for those organizations that are capable of adapting to a CMM-based management approach. SSE-CMM, in particular, is sufficiently developed and mature as to be integrated with relative easy into an organization that is already making use of a CMM 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 limited to an audit-oriented audience.

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 survived 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 paper 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.

A. REFERENCES

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. Canal, Vicente Aceituno. *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. Committee Sponsoring Organizations of the Treadway Commission (COSO). *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. Herzog, Pete. *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. International Organization for Standardization (ISO/IEC). *ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management.* Geneva: ISA, 2005.

18. International Organization for Standardization (ISO/IEC). *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. IT Governance Institute. *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. IT Governance Institute. *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. IT Governance Institute. *COBIT 3rd Edition Executive Summary*. Rolling Meadows: ITGI, 2000.

24. IT Governance Institute. *COBIT 3rd Edition Framework*. Rolling Meadows: ITGI, 2000.

25. IT Governance Institute. *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. IT Governance Institute. *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. IT Governance Institute. *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. IT Governance Institute. *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. IT Governance Institute. *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. National Institute of Standards and Technology. *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. National Security Agency. *INFOSEC Assessment Methodology: Modules 1 – 4*. Fort Meade: Undated, accessed 22 July 2004; available from http://www.iatrp.com/modules.cfm; Internet.

37. National Security Agency. *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.