A Unified Assurance Management Model

Journal:	*IEEE Security & Privacy*
Manuscript ID:	draft
Manuscript Type:	Regular
Date Submitted by the Author:	n/a
Complete List of Authors:	Tomhave, Benjamin; GWU, EMSE Ryan, Julie; GWU, EMSE
Keywords:	D.4.6.d Information flow controls < D.4.6 Security and Privacy Protection < D.4 Operating Systems < D Software/Software Engineer, H.0.a Infrastructure Protection < H.0 General < H Information Technology and Systems, H.1.0 General < H.1 Models and Principles < H Information Technology and Systems, K.4.4.f Security < K.4.4 Electronic Commerce < K.4 Computers and Society < K Computing Milieux, K.4.4.g Internet security policies < K.4.4 Electronic Commerce < K.4 Computers and Society < K Computing Milieux, K.4.4.i Economic and other policies < K.4.4 Electronic Commerce < K.4 Computers and Society < K Computing Milieux, K.6.4.b Management audit < K.6.4 System Management < K.6 Management of Computing and Information Systems < K Computing Milieux, K.6.m.b Security < K.6.m Miscellaneous < K.6 Management of Computing and Information Systems < K Computing Milieux

Proposed Title: A Unified Assurance Management Model

Benjamin L. Tomhave, M.S.
Julie J.C.H. Ryan, Ph.D.

Keywords

Abstract

Assurance organizations are increasingly challenged by the number of methods competing for attention; methods that can be classified as models, frameworks, and methodologies. The purpose of this research was first classifying these methods according to a defined taxonomy, then evaluating whether any such method could be used comprehensively and holistically across the enterprise. Failing that, this research then sought to combine key abstracted elements into a single unified approach. The result of this research was the development of the Total Enterprise Assurance Management (TEAM) model. Experts from the information security assurance field were asked to review and critique the model. Their feedback was integrated into the final draft of the model. This feedback from subject-matter experts was also used as an initial theoretical validation of the model. Future research efforts may include development of metrics and validation of the model in a real-world scenario.

1. Introduction

In the post-Sarbanes-Oxley environment of increasing regulatory mandate, a significant increase in the availability and composition of assurance methods has been seen. These methods purport to do any number of things, from providing step-by-step guidance for assessing the security of products to establishing an overall design for implementing security across the entire enterprise. In reviewing existing methods, however, it became clear that much confusion exists about these numerous methods and that there is no single method that can be cleanly overlaid across the full spectrum of enterprise assurance. Thus, after completing the initial literature review, the research took a natural progression into trying to define such a unifying, macro approach that could be used to manage the industry-preferred "best practices" approach within a given specialty area.

This research was conducted over 2005-2006, with the stated purpose of developing and validating a unified model that would position both industry and government strongly to harmonize competing assurance methods. This research was conducted in three phases. Phase 1 saw the collection and documentation of information assurance methods. Phase 2 created an overarching assurance management model. Phase 3 sought to have to have the overarching method created in Phase 2 validated by Subject Matter Experts (SMEs). As part of the validation performed in Phase 3, four hypotheses were tested:

- 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.

The significance of this research has been two key outputs. The first key output was the definition of taxonomy for classification of assurance methods and the subsequent classification of nineteen (19) methods within this taxonomic system. The second key output was the formulation of a unified model that brought together key aspects of information assurance management. This model takes a method-agnostic approach, providing implementers the flexibility to leverage a best practices approach, while still have central principles around which to be organized.

Key Terms

Before proceeding further, it is first important to level-set on terminology. Terms such as "information security," "information assurance," "governance," "audit," and "risk management" are increasingly nebulous and poorly defined. In this context, the term "assurance," or "information assurance," is used to describe the multiple core competency areas of "enterprise risk management," "operational security management," and "audit management." Each of these competency areas will be described in full later, as well as its central core organizing principle of policies. The purpose of defining these terms is to publish the lingua franca of this work, not to spur an academic discourse on the appropriateness of each definition.

- 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.

2. Overview of Literature Review

The Literature Review phase of research identified nineteen (19) assurance methods, which were then classified according to a taxonomic structure defined by the research. As defined in the overview, there were three classes within the taxonomy: Models, Frameworks, and Methodologies. These classes are listed in order from abstract to concrete.

Models were defined as being high-level, with minimal implementation concept. Instead, Models represent an abstract approach to information assurance that leaves the details of implementation open to interpretation. In contrast, Frameworks took a Model-like approach, but then extended the description to include guidance on implementation. Unlike Methodologies, however, the Framework stops short of procedural guidance and maintains a somewhat abstract view.

The methods identified through this initial research phase included majors like CoBIT, ISO 17799/27001, NSA IAM, NSA IEM, and so on. It should be noted that, while this research attempted to be as comprehensive as possible, it was inevitable that some methods would be missed. Furthermore, several other methods have emerged since completion of this phase of research. That being said, the results of this research still stand, unchanged. No methods identified in the intervening period provide a truly comprehensive, harmonized approach to assurance management.

One of the most important findings of Phase 1 was that only one true model was identified: The McCumber Model (or McCumber Cube). This model is not widely known, though its prevalence is increasing. What was unique about this method, versus others classified as Frameworks, is that it was abstract, generic, with potential applications to multiple aspects of information assurance, rather than addressing a specific purpose. Other methods, like ISO 17799/27001 came close to meeting the Model classification, but eventually failed the test due to containing significant implementation information (especially when one takes the entire 27000 series as one method).

The majority of methods identified fell into the Frameworks category, with Methodologies not far behind. This result is somewhat surprising, as one would expect more Methodologies. This expectation derives from the scoping of Methodologies as being targeted on performing a specific task. Given the more narrow scope of Methodologies, it would seem to descend naturally that there would then be a myriad of Methodologies around infinitesimal aspects of information assurance. Whereas this was not found in this phase of research, it is expected to be an emerging trend over time.

The initial purpose of this research was to identify an existing model that spanned all of assurance management, providing a flexible means for using a best practices approach in defining and implementing a program. The finding of only one actual model (McCumber) provided the first indication that no broad assurance management model might exist. A few framework candidates were considered in lieu of a model, but were eventually discarded. For example, CoBIT was primarily an audit framework, developed by auditors, with the intention of using the role of audit within the organization to force control objectives onto the business. The most recent revision of CoBIT has succeeded in lessening this audit-centric focus, but is still tainted by its origins.

The only framework that came truly close to being broad enough to encapsulate all of assurance management was the ISO 27000 series standards (including 17799, which is to be renumbered 27002). ISO/IEC 27001 was released in 2005, expanding upon ISO/IEC 17799:2000 (which was also released in an updated form in 2005). This standard goes through the process of defining an Information Security Management System, includes provisions for risk management and audit, as well as including details on identifying business requirements, regulatory requirements, and control objectives.

However, the ISO 27000 series fails in two areas by this research. First, it clearly falls into the Frameworks class, providing significant guidance for implementation, while also establishing a high-level approach. Second, while the standard purports to have flexibility – and does, in fact, advocate a flexible approach in defining requirements and controls – it is, in fact, a standard against which an organization can be certified. As a result of being certifiable, a certain degree of rigor and rigidity is implied that a true model would likely lack.

This aspect of the research – identifying numerous information assurance methods and classifying them according to a defined taxonomy – has been a useful output of the overall research process with potential for further development and refinement.

3. The Total Enterprise Assurance Management (TEAM) Model[1]

The Total Enterprise Assurance Management (TEAM) Model defines three core competencies within the overall category of information assurance management: Enterprise Risk Management (ERM), Operational Security Management (OSM), and Audit Management (AuM). These three competencies operate in a cyclical fashion, with the Universal Requirements Matrix (URM) being the hub to which their spokes connect. Figure 1 provides a visual representation of the overall lifecycle approach within the TEAM Model. In addition to the core competencies and URM, the model also introduces the key concepts of a policy framework (represented by the tilted, segregated gray triangle between ERM and OSM) and independence.

The key differentiators between the TEAM Model and a Framework such as ISO 27001 is that:
- … it allows, by definition, a flexible, best practices approach.
- … it is not a standard against which an organization can be certified.
- … it can be implemented in any size organization with minimal difficulty.
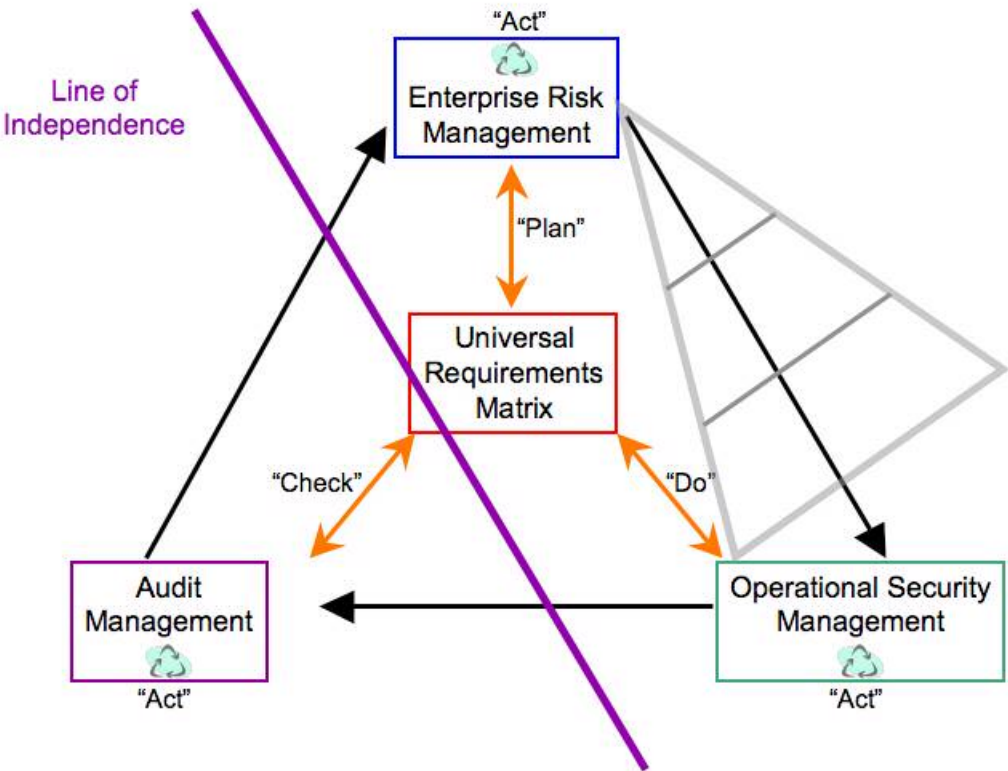- … it is extensible beyond the original scope defined.

Figure 1: The TEAM Model

The Universal Requirements Matrix

The single most important responsibility of an information assurance program is to define and understand business requirements. These requirements derive jointly from internal and external sources. Internal sources specify requirements for direction and performance of business. External sources generally account for regulatory requirements. Without first defining the requirements, it is then difficult - if not impossible - to chart an assurance strategy that accomplishes the goals of the business in the best manner possible.

In its simplest form, the Universal Requirements Matrix (URM) is a de-conflicted list of requirements that accounts for source of the requirement and priority for compliance. Stakeholders from all competency areas should be involved in the definition of the URM to ensure that requirements are feasible, and to help with conflict resolution.

As part of the URM definition process, all involved parties should decide upon a conflict resolution process. Establishment of such a process will be vital to the success of the URM definition phase. Conflicts between requirements will be inevitable as the regulatory environment evolves and becomes more complicated. For example, certain legacy systems will be technically unable to meet regulatory compliance, such as using secured communication protocols, without use of compensating controls.

Questions that need to be answered, as part of the conflict resolution process, should include:

- What is the cost of compliance?
- What is the cost of non-compliance?
- Which requirement represents a higher priority to the business?
- Are there compensating controls that can be used to side-step the conflict?

There are four functional purposes in defining the URM. First, definition of the URM clearly articulates the priorities of the business, to which all competencies can align. Second, the URM serves as direct input into the overall risk management approach, owned by the Enterprise Risk Management competency. How the URM is defined will have a direct impact on the risk management approach, including the sensitivity the business has to risk. Third, the URM also serves as a direct input for development of the policy framework. Fourth, the URM delineates the requirements against which the organization will be audited.

Figure 2 shows a general flow of requirements within the organization and the possible parallels to the policy framework. Note that business requirements and regulations are equal inputs into the top-level ("beginning") of the process. Audit feedback contributes to business requirements, as well as compliance activities. In addition to the downward, waterfall effect of standards disseminating within the organization, it is also significant to highlight the flow of feedback back up the organization.
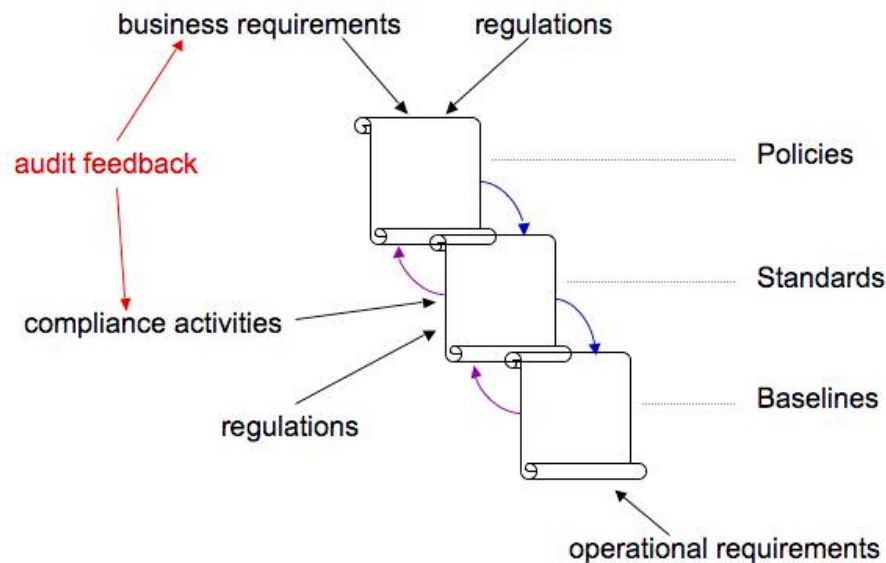

Figure 2: Flow of Requirements

Core Competencies

In performing the Literature Review in Phase 1 of the research it became evident that there were three general competency areas around which most methods were focused. Each competency area can be implemented according to a unique best practices approach and should leverage a lifecycle style in ensuring reiteration for efficiency and quality improvement over time. In cyclical order, the three competencies are: Enterprise Risk Management (ERM), Operational Security Management (OSM), and Audit Management (AuM). ERM feeds into OSM, which

feeds into AuM, which in turn completes the cycle by feeding into ERM. Each competency is described below, including its specific responsibilities with respect to the URM.

Enterprise Risk Management

Enterprise Risk Management defines the business-centric competency that is responsible for owning the URM, understanding the requirements imposed by the business and external entities, and translating these requirements into actionable directives, such as through the creation and propagation of policies. In essence, ERM represents the "plan" phase of the overall TEAM Model lifecycle.

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 an iterative lifecycle approach
- Adopts industry best practices, as appropriate
- Effectively "owns" the Universal Requirements Matrix
- Sets strategic direction for the 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

The Operational Security Management competency represents the implementation (or "do") phase of the lifecycle. OSM reads the requirements from the URM and policy framework, working towards a compliant position. In addition to implementing against the requirements, it is also incumbent upon this phase to provide feedback back to the ERM phase, such as in identifying requirement conflicts or requirements that are technically infeasible to implement.

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

Audi Management

The Audit Management competency area represents a key counter-balance to the ERM and OSM competencies, which essentially work together in defining and implementing the program. In addition to auditing the organization (OSM, in particular) for compliance with the URM, the

AuM competency also serves to ensure that the requirements themselves are aligned properly. Without AuM, the assurance program is without adequate controls, ensuring a consistent power struggle between ERM and OSM. As such, the AuM competency helps to mediate conflicts and provides assistance in determining if compensating controls can adequately address risks that may not be directly resolvable.

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

Policy Framework

As depicted in Figure 3, the policy framework has historically been hierarchical in nature, paralleling the Strategic/Tactical/Operational structure of the business. Policies are high-level statements that articulate strategic requirements and direction for the organization, from which everything else should descend. Policies lead to Standards, which exist at a more tactical than strategic level. Standards typically contain a mix of requirements and definitions, inline with the high-level requirements set forth in policies, but going into more detail. Well-written standards should contain enough information for implementation, though they should stop short of providing procedure-level guidance.

At the operational level of the organization then descends other forms of guidance that tend to be specific, detailed, narrow-focused, and technical. This level of documentation may be referred to as procedures, baselines, guidelines, or even frequently asked questions (FAQs).
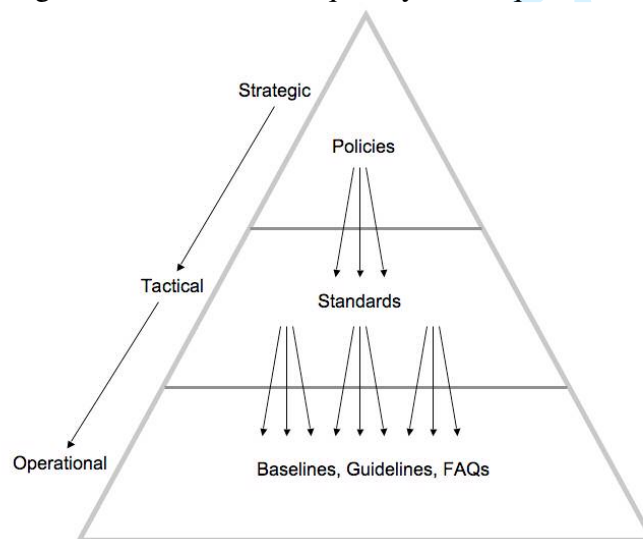

Figure 3: General Structure of Policy Framework

Within the context of the TEAM Model, the policy framework is owned by the ERM competency, much as the URM itself. However, in owning the policy framework, the ERM really has primary responsibility for the policies themselves, and then shares joint responsibility for standards, before relinquishing control of lower level guidance to OSM altogether.

In terms of the URM, it is important to note that requirements may exist within it at any level of the policy framework, from policy to standard to baseline or procedure. The level of the requirement will depend on the source. For example, some regulations (such as the Payment Card Industry Data Security Standard) provide very detailed and explicit operational requirements that cannot exist at a level higher than standards, and may in fact belong in a baseline or procedure document.

The Importance of Independence

Establishing and maintaining independence between the Audit Management competency and the other competencies of Enterprise Risk Management and Operational Security Management is imperative. The role of the auditor is to perform audit tasks checking for compliance with requirements and regulations. In order to objectively perform these audit responsibilities, the auditor must not have a vested interest in the definition and implementation of the requirements being audited against. Allowing auditors to have direct input into, for example, writing the policy framework represents a direct conflict of interest, since their independence will be relied upon in certifying audit results for audits performed against those policies.

In addition to the ideal purpose of objectivity and auditor independence, it is worth noting that this is a legal requirement, enforced in the United States via the Public Company Accounting Oversight Board (PCAOB), as sanctioned and authorized by the U.S. Securities and Exchange Commission (SEC). The audit function is a vital component to regulatory compliance; a function predicated upon the objectivity and independence of the auditors.

A Lifecycle Approach

Information assurance is a process, not a product or end-goal. This process includes the competency areas described above, covering the key bases of managing risk, securing the operational environment, and auditing for compliance. Toward that end, a lifecycle approach was defined so that enterprise assurance programs can evolve over time, improving with each iteration.

In addition to the need for iteration for continuous improvement, it is also important to note that requirements change over time. Businesses alter their strategies, regulations come and go, new threats and vulnerabilities emerge, and countermeasures change over time. In fact, about the only constant in the grand scheme of things is change. Thus, it's important to underscore the need for the lifecycle approach so that the wheels of the assurance model can keep pace with the rest of reality.

Beyond the macro lifecycle approach, it is also worth mentioning that each competency is free to implement its own lifecycle approach internally. One of the keys to the TEAM Model is that it allows each competency to identify and implement best practices within each competency. For

example, CoBIT may be appropriate for the Audit Management competency, while those in the Operational Security Management competency find that the NSA IA-CMM, IAM, and IEM are more suitable for their needs.

Regardless of approach used, each chosen high-level method should be cyclical in nature, reinforcing the journey rather than the short-term objectives. Given that the security environment changes dramatically over the course of each year, it is of the utmost importance not to get locked into one approach so tightly that it ends up suffocating the competency.

4. Overview of Subject-Matter Expert Analysis

Phase 3 of the research involved soliciting the feedback of subject-matter experts (SMEs) from throughout the information security industry. A cross-section of 24 reputable practitioners was selected, of which one (1) person opted entirely out of participating, one (1) person opted out of the formal survey, and eleven (11) participated in the full process, for a total uptake rate of over 45%.

The survey tool was designed primarily for use with a descriptive analysis, in part because of the small pool of respondents. Inferential analysis using Fisher's exact test was also performed. The survey instrument was not constructed for the purposes of performing an inferential analysis, nor was there a good dichotomy to identify, such as between adopters and non-adopters of the TEAM model. Nonetheless, the Fisher's exact test analysis provided additional insight into the results, as well as in identifying where future research could be focused.

Overall, feedback on the research was positive, with some indication that most of the hypotheses (described in Section 1) may have been achieved in the research. As a direct result of survey feedback, the thesis research was revised and improved. Following are some general highlights of the survey pertaining 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
- 46% thought it likely that they would implement the TEAM model when given the opportunity

In order to quantify SME biases, ranking tests were performed on the three (3) competency areas and the four (4) hypothesis objectives. The SMEs ranked the competencies as follows, from most to least important:
1. Enterprise Risk Management
2. Operational Security Management
3. Audit Management

SMEs ranked the hypothesis objectives in the following order, also from most to least important:
1. Better Management of Risk
2. Effectiveness
3. Efficiency
4. Optimized Operations

Based on the bias displayed above, SMEs were then asked a series of internally consistent questions on each specific hypothesis, with the following results:

- • H1a: Organizations that adopt a unified approach to information assurance will be more efficient than organizations that do not adopt a unified approach.
  - o 73% agreed that the TEAM model encourages efficient assurance management.
  - o 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.
  - o 63% agreed that the TEAM model encourages more effective assurance management.
  - o 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.
  - o 55% agreed that the TEAM model encourages better risk management.
  - o 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.
  - o 55% agreed that the TEAM model encourages optimized operations.
  - o 54% agreed that organizations adopting the TEAM model would optimize operations better than those that do not adopt a unified approach.

Shifting to the inferential analysis, the following results were calculated to determine if a relationship could be identified between specific questions. A finding was considered significant, and thus representative of a relationship, if Fisher's exact test produced a result in the range of 0-5%. In total, 37 tests were executed against the data, using both redacted (to remove non-committal answers) and original data sets. Each question objective is summarized with the corresponding 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

Overall, the inferential analysis primarily calculated 2-tail p-value results of 1, indicating that questions had no relationship whatsoever. Since the tests were not constructed with an inferential analysis in mind, this result was not surprising. Additionally, since there was not an implementation of the TEAM Model, there was no easy way to separate the respondents into two distinct groups. 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 stipulated.

This conclusion is contradictory to the descriptive analysis. However, again, because of the softness of the inferential analysis, this result is neither surprising nor conclusive.

5. Conclusions and Future Research

In general, subject matter experts and the community at large deemed the research beneficial. The production of a taxonomy and reasonably exhaustive list of information assurance methods filled a void in the industry and academia. Furthermore, the TEAM Model introduced a new work to the overall collection of methods that was unique and flexible.

Feedback on the work was received positively. The survey results were not adequate to draw firm conclusions, but provided an early indication that most of the research was successful.

Future research could be done in the following areas:
- Revision and expansion of the base Literature Review, such as through adding more methods and broadening research into applicable regulations.
- An enhanced, general population survey seeking feedback on the TEAM model, with particular construction to facilitate an inferential analysis.
- Implementation of the TEAM Model within an organization.
- Integration of the TEAM Model with management approaches such as balanced scorecard.
- Identification of metrics for measuring effectiveness, efficiency, impact on risk management, and impact on optimizing operations to support or refute this research.

References

1. Tomhave, Benjamin L. *The Total Enterprise Assurance Management (TEAM) Model: A Unified Approach to Information Assurance Management*. Fairfax: Benjamin Tomhave, 2006, accessed 31 December 2006; available from http://falcon.secureconsulting.net/professional/papers/Tomhave_Thesis-FINAL.pdf; Internet.