USF | Muma Business Review
A publication of the Muma College of Business | University of South Florida

Volume 1, Number 13 | Research Question Review | 1 SEPTEMBER 2017

# What Factors Influence Companies' Successful Implementations of Technology Risk Management Systems?

By
Ed Fulford, University of South Florida

During the initial literature review on this research question, areas of focus included the following:

- Current qualitative and quantitative methodologies for technology risk analysis.
- Business applications for expanding the use of qualitative and quantitative technology and security risk models.
- Implementation of qualitative and quantitative technology and security risk analysis methodologies models by practitioners.

Information Technology (IT) risk analysis has become be an integral part of the enterprise risk management systems in many organizations. However, many companies have struggled to effectively implement these systems. This has become a serious problem in many cases where governmental regulations, industry requirements, and even contractual language for doing business have increasingly included technology risk management obligations that companies must meet. Currently, technology risk management is not as mature a field as those like IT Audit or Information Security, which have had professional certification processes for over 23 years. Technology risk management, on the other hand, has had similar certifications for less than 10 years. As such, many of the current technology risk management practitioners have come from other fields, which has made it difficult to construct a common body of knowledge on which technology risk management systems can be built. In many cases, such factors, as well as others, are making it difficult to implement technology risk management systems. This research will seek to evaluate those factors in more detail to determine common ones that have the most impact on the success of technology risk management projects and make recommendations for overcoming the factors that limit the success of these projects.

**As the Information Technology (IT) networks and systems used in business becomes more interconnected and intricate, research considers how risk management methods can identify critical technology and security risks, and determine the potential effects on the company should those risks be exploited.**

**Keywords:** Quantitative Risk Models, Qualitative Risk Models, Risk Analysis, Risk Management, Technology Risk Management System.

## Introduction

Information Technology (IT) risk analysis has become a significant and growing part of enterprise risk management programs in many corporations. In general, this is due to the potential effects on corporations--financial, operational, and reputational--when risks to increasingly complex IT networks and systems are exposed by security or technology-related events. However, the technology risk analysis literature suggests that many of the assessment methods that are currently used by practitioners in the field are qualitative processes based on expert knowledge. In most cases, these methods do not leverage the more quantitative approaches developed and tested through academic research. This research question will seek to discuss the challenges companies face when implementing technology risk management methodologies, and which of the techniques--quantitative or qualitative--are more successful when deployed. It is also an attempt to draw initial conclusions on which approaches to implementing technology and security risk management methodologies are most effective in helping organizations deal with these issues. Additionally, this work will begin to lay a foundation for further investigation on the most effective ways to successfully implement the risk analysis methodologies by IT risk management professionals. This research can provide further insights on those techniques that can be used to determine the effectiveness of newly deployed enterprise technology risk management systems.

## Research Questions

One of the goals of this research project is to define and validate a conceptual model that describes or explains the forces affecting the successful implementation of technology risk management systems. To accomplish this goal, the research activities will focus on answering the following explanatory questions:

- What are widely-accepted technology risk management methodologies that have been

## Methodology

The study will attempt, using a number of online databases, to identify specific academic and practitioner literature sources that discuss the implementation of technology risk management systems for different organizations. Primary focus of this effort is to gather a variety of academic, government, and industry experiences and insights on implementing technology risk management systems to delve more deeply into the scope of these types of projects, and the factors that challenged the entities managing the implementations to completion.

As part of this literature review, the author also attempted to determine if there were specific management theories that could be applied to assist in the understanding of the factors that influence the successful implementation of technology risk management systems. As such, the author researched several such theories in order to define a conceptual model that could help explain factors noted as key influencers to implementing management strategies and methodologies, and see if those would have similar effects in technology risk management system projects.

Once the articles are selected, the articles will be examined. The key factors regarding the selection and implementation of technology risk management systems will be categorized and examined to determine common themes and other characteristics of successful implementations of technology risk management systems.

Articles were selected for further review based on both the type of technology risk management methodology being utilized as well as any additional information on the success or failure of its implementation. Initial research considerations for including articles in the literature review included the inherent complexity of the technology risk management system, its current level of adoption, and practitioner comments about the specific technology risk management systems utilized in the organization.

### Databases Used

In the initial literature review on the development and types of technology for security risk management methodologies and models--ABI-Informs, Google Scholar and JSTOR.org were used for those searches. These databases were selected as excellent starting points for the literature review, based on the recommendations of the USF librarians and the DBA program's professors.

The queries to these databases found a significant body of literature on these subjects by both academics and practitioners, with articles and books dating from the 1990s. These are the selected results of the database queries. Further review and summarization of the referenced articles and books are planned to refine future queries as part of the ongoing research.

proposed in literature or are being deployed in practice?
- How do security/risk practitioners implement technology risk management methodologies in their companies?
- What are the forces that drive the selection of a technology risk management methodologies in a company?

## Proposed Conceptual Model

In the Proposed Conceptual Model (see Figure 1), the research will seek to articulate the vertical and horizontal forces that influence successful technology risk management system implementations. There is competition for resources within these projects as the corporate business strategy helps identify its risk posture, and how that posture can be managed and measured. These forces have varying impacts on the implementation project as the different approaches to technology risk management are evaluated. In the Conceptual Model, the vertical force of Alternative Risk Management Strategies are investigated to ultimately select the Technology Risk Management Methodology that fits the corporate strategic and operational requirements.

These two vertical forces (Technology Risk Management Methodology and Alternative Risk Management Strategies) contend for resources required to implement the selected risk management methodology (see Figure 1). The forces impact the company's ability to measure risk and show the company's overall risk posture is being managed effectively. If these risk management systems are changed, the company is typically required to reassess its risk posture and how that change impacts its operational stance. In this way, the Proposed Conceptual Model would predict that any change in the forces will typically require a business to re-assess its technology risk posture with respect to the overall change in its technology footprint it uses to support its strategic and operational decisions and initiatives.

The vertical forces on the corporation's internal technology environment are ways that the stakeholders influence the direction and scope of the technology risk management systems implementation. These influencers provide internal context on how the selected Technology Risk Management system is implemented, how its success is measured, and how it is evaluated against Alternative Risk Management Approaches (such as internal or external audits, external risk assessments, or regulatory reviews).

As horizontal forces, Risk Management Practitioners (see Figure 1) influence the technology risk management system implementation by providing the subject matter expertise on risk management, and the specialized knowledge of the various technologies in use within the company. This grounding enables them to configure the technology risk management

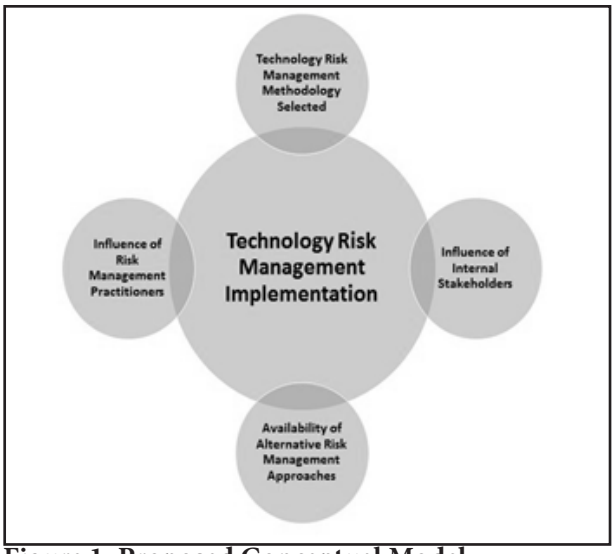


**Figure 1: Proposed Conceptual Model**

system to provide the key performance metrics and reporting required by management.

The influence of Risk Management Practitioners is a key force in providing the necessary resources (in this case, the subject matter expertise and knowledge) to successfully implement the technology risk management system. Should the Risk Management Practitioners not be available or not have sufficient technical knowledge in technology risk management, the overall implementation project will not be as successful as it could be--much like a company not being able to enter a key market if it cannot engage the right suppliers.

Other horizontal forces include Internal Stakeholders (see Figure 1), who have a very different effect on the success of the implementation of the technology risk management system. They can influence many of the business and cultural factors that will aid in both the success of the implementation and its long term acceptance. The technology risk management system is the "product" for assessing the corporate risk posture and the Internal Stakeholders are the "market" for that product.

As the Internal Stakeholders are engaged by the Risk Management Practitioners about the types of technology risk management systems to implement, the Internal Stakeholders can provide not only input over the system itself, but other important feedback on how the system can be used within the corporation and affect its culture, operations, and strategy. As the "market" in a sense for the technology risk management system, the Internal Stakeholders want the technology risk management system to be the right business and right cultural fit. This desire is often critical to the success of the overall risk management system. Should these two requirements be either ignored or downplayed by the Risk Manage-

ment Practitioners, the technology risk management system implementation is likely to be delayed, not accepted by its "market", or fail altogether. The end result is the company has likely created a management reporting void for risk analysis, and reporting that will take a significant amount of time, investment, and cultural adjustment to overcome.

## Key Terms for the Forces Used in the Proposed Conceptual Model Include:

- **Internal Stakeholders:** those entities inside the organization that support or are recipient of outputs from the technology risk management methodology.
- **Risk Management Practitioners:** those entities that manage and report on the effectiveness of the technology risk management methodology.
- **Risk Management Methodologies:** those analytical techniques (often based in software), performance measurements, and remediation practices that allow Risk Management Practitioners to assess, categorize, prioritize, and assist in the remediation of technology risks in the organizations.
- **Alternative Risk Management Strategies:** management practices for managing technology risks, including risk acceptance, that are used in lieu of a technology risk management methodology.
- **Technology Risk Management Implementation:** the process through which a company selects, plans, and deploys the technology risk management methodology.

# Literature Summary

The initial literature review consisted of a survey of a number of technology risk management systems. The first part of the research sought to quantify the number of generally accepted technology risk management systems that were used by practitioners, to

**Table 1: Literature Comparing Different Technology Risk Management Systems**

| Sources | Findings |
|---|---|
| Aagedal, J. Ø., Den Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D., & Stølen, K. (2002). Model-based risk assessment to improve enterprise security. In *Enterprise Distributed Object Computing Conference, 2002. EDOC '02. Proceedings. Sixth International* (pp. 51-62). IEEE. | • CORAS is the name of a European research and technological development project which aims to produce an improved risk analysis methodology for systems where security is a critical requirement (p. 51).<br>• CORAS builds on other complementary risk management methodologies such as the HAZard and OPerability study (HazOp), Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA), Markov analysis, and CCTA Risk Analysis and Management Methodology (CRAMM) (p. 51).<br>• In use, CORAS can provide an excellent way for different groups of stakeholders involved in a risk assessment to communicate and interact, which can improve the effectiveness of the assessment and provide risk feedback to system designs (p. 60). |
| Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM. | • Evidence increasingly indicates that information security technology does not effectively reduce information risk (p. 97).<br>• There is no current literature showing any current information security standard which mandates the use of a quantitative risk analysis method (p. 99).<br>• Collecting information risk data needs to be more regular, formal, and comprehensive in order to better assess information risk (p. 102).<br>• Information security risks will continue to be poorly understood until economic losses can be quantified more accurately (p. 103). |
| Eloff, J. H., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, *12*(6), 597-603. | • CCTA risk analysis and management methodology (CRAMM) was developed by government to identify and justify controls and other protective measures related to the security of IT systems used to process unclassified but sensitive information (p. 600).<br>• Los Alamos Vulnerability/ Risk Assessment (LAVA) is a systematic methodology for assessing vulnerabilities and risks in complex safeguard and security systems, and was created to address complex systems that are too large for other risk analysis methods (p. 601).<br>• Because CRAMM and LAVA vary in their coverage of technology risk areas, it is advised that these methods be used in conjunction with other ones for the initiation, but also for the management of an information security risk management program (p. 602). |

**Table 1 (Continued)**

| Sources | Findings |
|---|---|
| Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information security and applications*, *18*(1), 45-52. | • There is a significant body of literature on current ISRA methodologies, but additional research is required because standardized and trustable ISRA methods are not available to organizations (p. 47).<br>• The majority of ISRA methods are proprietary, which limits an organization's ability to select a suitable one (p. 47).<br>• A majority of the risk management methodologies do not provide for risk management projects that include tasks such as training, workshops, updating of risk registers, risk monitoring, and risk reassessment (p. 50). |
| Vorster, A., & Labuschagne, L. E. S. (2005, July). A framework for comparing different information security risk analysis methodologies. In *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 95-103). South African Institute for Computer Scientists and Information Technologists. | • Five different information security risk analysis methodologies were analyzed, and the way in which each of them analyzes risk was investigated (p. 95).<br>• The proposed framework was developed by analyzing five other methodologies in detail and identifying some common criteria, which were then used to form the criteria of the proposed framework (p. 102).<br>• The advantage of the proposed framework is its ability to eliminate the unsuitable methodologies and to only further investigate the remaining ones (p. 102). |

determine what types of systems (qualitative, quantitative, or a hybrid of the two) were used. During this research, over 15 different technology risk management systems were identified for further evaluation (see Table 1). Approximately 80% of these systems were developed by practitioners, and the other 20% were created as part of academic research.

The second part of this review dealt with searching the academic literature for any articles on the implementation of the technology risk management systems identified. Selected articles on qualitative technology risk management systems are listed in Table 2 and literature reviewed on quantitative technology risk management systems is highlighted listed in

**Table 2: Literature Discussing Qualitative Technology Risk Management Systems**

| Sources | Findings |
|---|---|
| Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Boston: Addison-Wesley Longman Publishing Co., Inc. | • Many risk evaluation methods do not review and analyze risks to an organization's mission and business strategies.<br>• The OCTAVE methodology helps an organization understand its most important information, technology, and other assets, and what risks can threaten those assets.<br>• Most of the risk evaluation in OCTAVE is qualitative, based on domain expertise and knowledge. |
| Coles-Kemp, L., & Overill, R. E. (2007). On the role of the facilitator in information security risk assessment. *Journal in Computer Virology*, *3*(2), 143-148. | • The Information Security Management standard ISO 27001 mandates that a formal risk assessment is undertaken in order to manage and maintain an Information Security Management System (ISMS) (p. 143).<br>• The Facilitated Risk Analysis and Assessment Process (FRAAP) is a qualitative risk assessment process where the key feature is that the business drives the risk assessment process, and the security risk analyst acts as a facilitator (p. 145). |

**Table 2 (Continued)**

| Sources | Findings |
|---|---|
| | • The effective facilitator of a FRAAP assessment requires a knowledge of systems and business process modelling, a range of tools and methodologies for assessing business problems, an ability to translate risks between the different layers in an organization, a teacher's approach to risk assessment, and a detailed knowledge of risk analysis practices (p. 147).<br>• FRAAP builds on traditional risk assessment methodologies, which were created to help evaluate computer security and risk issues, and address increasingly complex information security management challenges that impact business processes (p. 148). |
| Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. Risk management guide for information technology systems. | • The guide describes the risk management methodology, how it fits into each phase of the Systems Development Life Cycle (SDLC), and how the risk management process is tied to the process of system authorization (or accreditation in government systems) (p. 4).<br>• A risk management program requires senior management's commitment, support and engagement from the Information Technology (IT) organization, the competence of the risk assessment team to apply its methodology, the cooperation of user stakeholders, and an ongoing evaluation and assessment process of the IT-related mission risks (p. 41). |
| Wawrzyniak, D. (2006). Information security risk assessment model for risk management. In *Trust and Privacy in Digital Business* (pp. 21-30). Springer Berlin Heidelberg. | • Information Security has become an interdisciplinary task that takes advantage of many sciences including the organizational and economical ones as well as statistics and mathematics (p. 21).<br>• The Financial Services Roundtable KALCULATOR model takes advantage of simple quantitative tools, where there are others like ISRAM and Return on Security Investment (ROSI) that use more sophisticated mathematical and statistical analyses (p. 23).<br>• Risk decisions are based mainly on the historical data dealing with the specific security threats and their business impacts, and not only on expert knowledge (p. 30). |

Table 3. The use and benefits of the particular systems were often the focus of the articles. There was little information on the success of implementing these systems as part of corporate risk management programs, which provided the researcher with the ideas for future research questions and literature reviews.

**Table 3 - Literature Discussing Quantitative Technology Risk Management Systems**

| Sources | Findings |
|---|---|
| Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Boston: Addison-Wesley Longman Publishing Co., Inc. | • Many risk evaluation methods do not review and analyze risks to an organization's mission and business strategies.<br>• The OCTAVE methodology helps an organization understand its most important information, technology and other assets and what risks can threaten those assets<br>• Most of the risk evaluation in OCTAVE is qualitative, based on domain expertise and knowledge. |
| Chaudhuri, A., & Ghosh, S. K. (2016). Operational Risk. In *Quantitative Modeling of Operational Risk in Finance and Banking Using Possibility Theory* (pp. 7-28). Switzerland: Springer International Publishing. | • Under Basel Committee guidelines, banks must establish an independent operational risk management and control processes (which includes the review of technology and security risks). This includes establishing the measurements for operational risks and controls (p. 20).<br>• Banks must consider whether a technology control is truly reducing risk, or merely transferring exposure from the operational risk area to another business sector (such as the use of cybersecurity insurance) (p. 21).<br>• Firms were using or considering using insurance policies to mitigate operational risk because of the difficulty in measuring the impacts from risks (p. 22). |

**Table 3 (Continued)**

| Sources | Findings |
|---|---|
| Cheng, P. C., Rohatgi, P., Keser, C., Karger, P. A., Wagner, G. M., & Reninger, A. S. (2007, May). Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *Security and Privacy, 2007. SP'07. IEEE Symposium on* (pp. 222-230). IEEE. | • Quantified risk–adaptive access control (QRAAC) may help address issues that exist in current access control systems (p. 2).<br>• Many factors contribute to risk and it may be difficult to design one formula covering all factors (p. 6).<br>• Such a formula will contain many tunable parameters and be difficult to maintain (p. 6). |
| de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*(1), 25-34. | • The proposed fuzzy decision-based method evaluates scenario-based sequences of events (referred to as alternatives) in information security incidents (p. 25).<br>• The taxonomy developed assists in the criticality ranking of alternatives using Event Tree Analysis (p. 30).<br>• Probability models built upon classic set theory may not be able to describe some risks in a meaningful and practical way, hence the use of fuzzy set theory (p. 27). |
| Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*(2-3), 203-225. | • To have a systematic study of e-commerce security issues, an organized classification that helps our understanding of threats is needed (p. 204).<br>• An evaluation system is being developed incorporating the aspects of electronic commerce and vulnerability assessment to develop a framework for addressing security risk assessment issues in organizations (p. 220).<br>• Using decision models requires security management to become more aware of the security issues impacting these analyses (p. 222). |
| Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, *256*, 57-73. | • The Security Risk Analysis Model (SRAM) uses techniques such as Bayesian networks and colony optimization in development of risk analyses (p. 58).<br>• SRAM has three phases including Bayesian network development, security risk assessment, and vulnerability propagation analysis (p. 60).<br>• Some potential issues with SRAM include the updating of event probabilities and the expanding capability requirements in the analysis of network vulnerabilities (p. 69). |
| Freund, J., & Jones, J. (2015). *Measuring and managing information risk: A FAIR approach*. Oxford: Butterworth-Heinemann. | • The Factor Analysis of Information Risk (FAIR) methodology was developed to assist companies in measuring and managing information risk.<br>• FAIR has been adopted by many companies and provides a proven framework for understanding, measuring, and analyzing information risk in organizations of many sizes and complexities. |
| Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16-30. | • The quantification of risk to physical or tangible assets has proved difficult (p. 17).<br>• Risk estimation, including its probability of occurrence and severity of impact, requires extensive domain expertise and knowledge (p. 22).<br>• The proposed view for risk management borrows from natural science, theoretical science, and social science research methods, attempting to quantify risks on both tangible (like computers) and intangible Quantified Risk-Adaptive Access Control (QRAAC) assets (like information) (p. 28). |

**Table 3 (Continued)**

| Sources | Findings |
|---|---|
| Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147-159. | • The Information Security Risk Analysis Method (ISRAM) is proposed for information security risk analysis by encouraging the participation of management in the analysis of risks to complex systems (p. 148).<br>• ISRAM has a quantitative component which relies on surveys for creating its data model and associated risk analyses (p. 150).<br>• ISRAM uses basic mathematical models to analyze risk data, but with no statistical components. |
| Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., De la Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, *39*(4), 774-784. | • Accumulating the number of security incidents that are detected, through any detection mechanism or process measures only a percentage of the true incident rate, and that percentage is unknown (p. 775).<br>• In correlating expert judgment on a survey on security protection and control as inputs, a weighted average of those inputs is often used, and a significant amount of research has centered on determining an appropriate weighting scheme for the inputs (p. 776).<br>• Statistical information that can be used for quantitative risk management evolves so slowly that it cannot keep up with the evolution of the threat environment (p. 783).<br>• The research showed that a competently managed system with no security protections is slightly less likely to have a successful attack, but that advantage drops off over a longer term (p. 783). |
| Sommestad, T., Ekstedt, M., & Johnson, P. (2010). A probabilistic relational model for security risk analysis. *Computers & security*, *29*(6), 659-679. | • Analysis frameworks may restrict themselves to a limited number of variables, which can blur the understanding of dependencies among the properties of risk treatments, the threat environment, and sensitive assets (p. 660).<br>• Probabilistic Relational Models (PRMs) can be utilized for security risk analysis because they contain classes, attributes, and class-relationships that can be extended to risks under review (p. 660).<br>• The versatility provided by the probabilistic aspects of PRMs makes it possible to specify security theories on any abstraction level (p. 677). |
| Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), 45-56. | • It is very difficult to obtain data about the true cost of a security incident because few companies successfully track security incidents (p. 57).<br>• With a good survey and scoring system for productivity, combined with external measurements of intellectual property value, it becomes possible to quantify risk exposure in a repeatable and consistent manner (p. 60).<br>• Even with an inaccurate scoring algorithm, using a scored assessment as a method of determining risk mitigation is effective because the scores are repeatable and consistent, and therefore can be used to compare the Return on Investment (ROI) of different security solutions (p. 62).<br>• The SecureMark system discussed is an implementation of the risk management concepts designed to provide a standard for security benchmarking, to produce repeatable results that are correlated to financial performance (p. 64). |
| Verendel, V. (2009, September). Quantified security is a weak hypothesis: A critical survey of results and assumptions. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 37-50). ACM. | • There is a significant body of work about quantified security, but the evidence does not seem to indicate that the methods used accurately represent security in operational settings (p. 37).<br>• Many quantitative methods use assumptions about operational security that are neither obvious to practitioners nor thoroughly tested empirically (p. 44).<br>• The result from reviewing many of the methods is that the hypothesis that operational security can be quantified is weak (p. 46). |

The third part of the study was performed to investigate the researcher's thinking on a Proposed Conceptual Model for setting the research questions. Upon a recommendation in a peer review, the researcher began to search for information on Porter's Five Factor Analysis Model (see Table 4). The Porter Model served as the starting point for the Proposed Conceptual Model, which identifies key forces that factor into the successful implementation of technology risk management systems. Additional literature reviews will be performed to determine the correlation of Porter's model to the researcher's Proposed Conceptual Model.

## Discussion

From this literature review, it is clear that the problem of effectively implementing robust methodologies to quantify technology and security risks has existed for as long as governments and businesses have been using computers, application software, and networks. To address this problem, qualitative and quantitative risk analysis models have been developed by both academics and practitioners with varying degrees of implementation by government agencies and industry segments, though government has led industry in such implementations.

One significant difference in the academic and practitioner models is that academic researchers have created statistical mathematical models to evaluate risks in specific security domains like access control and network vulnerabilities, which are complex and difficult to implement on a wider scale (see Table 5). By comparison, practitioner models have been designed to analyze multiple types of risks across several security domains, and are based on expert knowledge instead of statistical models (see Table 5). Academic research in this area has been attracting more attention because of the growing number of cybersecurity breaches and related incidents.

At this time, many of these academic models are mathematically and statistically complex and are not easily understood and, as a result, not implemented by practitioners. Practitioners have also responded to this increase in the risk landscape by adopting

**Table 4 - Literature Discussing Strategy Development Using Industrial Organization Economics**

| Sources | Findings |
|---|---|
| Porter, M. (1981). The contributions of industrial organization to strategic management. *The Academy of Management Review,* 6(4), 609-620. Retrieved from http://www.jstor.org/stable/257639 | • The goals of the firm were broadly conceived to encompass both economic and non- economic considerations, such as social obligations, treatment of employees, and organizational climate (p. 610).<br>• Industrial Organization (IO), by and large, viewed the firm as a single decision-making unit making choices based on economic objectives (p. 612).<br>• Increasingly, IO research is beginning to encompass dynamic models of industry evolution, some framed from the point of view of the strategic decision facing the individual firm (p. 615). |
| Porter, M. E. (2008). *Competitive strategy: Techniques for analyzing industries and competitors*. New York: Simon and Schuster. | • Survival of the organization lies in creating a best fit between environment and resources of the organization.<br>• The structure of industry and environmental forces keep on evolving, thereby forcing organizations to consistently interact and respond according to the changing environmental conditions.<br>• The book provides a framework of relating a company to its environment. Framework encompasses a best fit between firm's resources and environment. |
| Yamin, S., Gunasekaran, A., & Mavondo, F. T. (1999). Relationship between generic strategies, competitive advantage and organizational performance: An empirical analysis. *Technovation*, *19*(8), 507-518. | • In the industrial organization and business strategy literature, considerable interest has been centered on identifying generic business strategies or strategy types based on strategy components, such as the scope or domain of the business, resources deployment in marketing, production and R&D, asset management or parsimony, and degree of vertical integration (p. 507).<br>• The notion underlying the concept of generic strategies is that competitive advantage is at the heart of any strategy, and in order to attain competitive advantage the organization has to make a choice about the type of competitive advantage, it seeks to attain and the scope within which it will attain it (p. 509).<br>• A broader conceptualization of business performance would include emphasis on indicators of operational performance (i.e., nonfinancial) in addition to indicators of financial performance (p. 510). |

hybrid quantitative/qualitative risk management models. These are generally made for ease-of-use, and rapid identification and enumeration of risks, with minimal quantification and statistical evaluation of the potential events and their impacts. A middle ground of more mathematically and statistically based risk models that are still relatively easy for practitioners to understand and implement is an emerging paradigm which is being considered by the firms that develop commercial technology risk management systems. This will bring the academic methodologies closer in their application to the practitioner ones, though there will still be significant differences in the ways those two groups approach implementing technology risk management systems.

As shown in Table 5, several of the differences could be challenges in the applicability of academic and practitioner technology risk management methodologies. In general, academic technology risk management methodologies are more customized, and often focused on a very small part of the technology footprint that an entity would implement. In a number of articles reviewed, the focus was network infrastructure. Network devices generate a large amount of data for researchers to model and study, making them an attractive area for research.

Practitioner methodologies, on the other hand, are broader in their scope. They are often based on corporate requirements to help senior management understand the technology risks their companies face in a concise and understandable fashion. Additionally, these methodologies are often worksheet or questionnaire based, which allows for the practitioner to add comments based on expert knowledge, making further statistical analysis more difficult or impractical because many of the responses to the technology risk assessments are opinions or observations, instead of mathematical data.

The number of differences that exist between academics and practitioners when it comes to the ways that each group approaches technology risk management methodologies has been decreasing. However, there are relatively few similarities on how these methodologies are implemented at this time. There is, as mentioned above, a trend among technology security and risk management practitioners to create hybrid models that contribute both qualitative (expert knowledge) and quantitative (data analytics) into the technology risk management systems they implement, but this hybrid approach is still relatively new to the industry. As such, there is a potentially compelling area of practitioner-focused research that can help security and risk professionals to better understand how to utilize data analytics in their risk management methodologies, and to effectively implement those quantitative methods by defining key performance measurements and indicators.

## Limitations of Current Research

It can be very challenging for researchers to find suitable companies to investigate how the organizations implement technology risk management systems. In many cases, companies (especially in highly regulated industries like Financial Services and Healthcare and in government agencies) have contractual, industry, or other legal restrictions that limit their abilities to consent to this type of research and then permit the researchers to publish their findings.

If researchers are allowed to work with firms to

**Table 5: Differences between Academic and Practitioner Approaches to the Implementation of Technology Risk Methodologies**

| Differences | Academic Approach | Practitioner Approach |
|---|---|---|
| **Type of Technology Risk Model** | Quantitative | Qualitative or a Hybrid of Qualitative and Quantitative |
| **Primary Technology Risk Measurement Technique** | Custom Application | Interview, Questionnaire, Commercial Application |
| **Technology Risk Measurement Process** | Statistical | Expert Knowledge |
| **Primary Technology Risk Focus** | Validation of Research | Impact on IT or Business Operations |
| **Primary Security Domain Assessed** | Access Control, Network Infrastructure, Technical Vulnerabilities | Multiple Technology Domains (Applications, IT Operations, Network Infrastructure, Third Party Technology Partners) |
| **Organizational Implementation** | Not Evaluated | Important |

study how technology risk management systems are selected, implemented, and utilized, they will typically be required to sign non-disclosure or confidentiality agreements. The language in these documents can further restrict the researchers' access to key personnel and use of pertinent information. Both of these items can limit the scope of the research and the researchers' ability to publish the outcomes of their inquiries in academic journals and practitioner periodicals.

Because of the issues noted above, it is relatively difficult for researchers to both conduct in-depth investigations into how companies implement technology risk management systems and to then publish the findings. As such, it would be hard to generalize the results from these studies to specific industries or types of companies. Additionally, as this literature review discovered, there is lack of academic articles and other publications on how companies or government agencies implement technology risk management methodologies. In approaching this topic and beginning to investigate it further, the researcher will not be able to build on the work done by others, which can increase the time required to perform this study.

## Conclusions

The differences identified between academic and practitioner technology risk management methodologies indicate these dissimilarities potentially can affect how the methodologies are implemented. However, there is little discussion in the literature about why implementation of the various methodologies, especially the ones developed by academics, are either not successful, or are not deployed in practice. Additional research will explore which widely-accepted technology risk management methodologies are being deployed in practice, and why those systems are implemented successfully. Also, investigation into the various forces that impact these implementations will be evaluated to determine if an effective conceptual model, such as the one proposed here, can accurately describe the impact of these forces.

The initial literature review provided a number of interesting insights about the development, implementation, and use of technology risk analysis and assessment models. There is general agreement in the literature that it is difficult to quantify technology and security risks because identifying and evaluating the risks requires significant domain expertise and knowledge. The quantitative risk analysis methods currently in use vary and are often based on the types of risks evaluated (such as access control, information risks, and technical vulnerabilities), and the ways the risks are modeled (statistical analysis versus experience-based scoring based on practitioner observation).

Qualitative risk management methodologies, while more easy to implement and use, are now being seen as less effective in providing companies with accurate performance indicators and metrics. It is increasingly difficult for practitioners to assess and observe security and technology risks, especially in the areas of application development, network management, and security event logging. Without having a risk management system with more quantitative capabilities to perform data analytics on technology elements like computer source code for enterprise applications and system logs from a widely deployed network infrastructure, practitioners cannot create key performance and risk indicators, and communicate any inherent and residual risks.

Conclusions drawn from comparisons of the technology risk management methodologies and models investigated during the literature review included:

- Some risk analysis methods (such as CORAS and FAIR), utilize design aspects from other risk methodologies and are very complementary with those methodologies in use (see Table 1).
- Practitioners have developed models that typically do include quantitative methods, but these generally lack a mathematical analysis component, such as a statistical model, which limits the ability of those models to determine the relationships and impacts of security and technology operational risk events to IT operations (see Table 2 and Table 5).
- Practitioner models are typically constructed for experienced users with extensive domain knowledge (see Table 2 and Table 5).

Qualitative risk management methodologies, while more easy to implement and use, are now being seen as less effective in providing companies with accurate performance indicators and metrics.

Other conclusions drawn during the literature review are:

- There is limited literature showing that some of the more theoretical quantitative methods developed by academics are finding acceptance and implementation by practitioners.
- There is limited literature suggesting that academic and practitioner models are being combined to create more comprehensive, mathematically-based ones and then implemented successfully.
- There is limited literature on the effects on organization of the implementation of quantitative technology and security risk models over time.

After the initial round of the literature review, no information on the effectiveness and implementation of these models by industry and government organizations was found through the searches utilized. As such, more sophisticated queries need to be developed to determine if there is more literature on practitioners' expert opinions regarding these models, and their current and potential usefulness.

## References


Aagedal, J. Ø., Den Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D., & Stølen, K. (2002). Model-based risk assessment to improve enterprise security. In *Enterprise Distributed Object Computing Conference, 2002. EDOC'02. Proceedings. Sixth International* (pp. 51-62). IEEE.

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Boston: Addison-Wesley Longman Publishing Co., Inc.

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.

Chaudhuri, A., & Ghosh, S. K. (2016). Operational Risk. In *Quantitative Modeling of Operational Risk in Finance and Banking Using Possibility Theory* (pp. 7-28). Switzerland: Springer International Publishing.

Cheng, P. C., Rohatgi, P., Keser, C., Karger, P. A., Wagner, G. M., & Reninger, A. S. (2007, May). Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *Security and Privacy, 2007. SP'07. IEEE Symposium on* (pp. 222-230). IEEE.

Coles-Kemp, L., & Overill, R. E. (2007). On the role of the facilitator in information security risk assessment. *Journal in Computer Virology*, *3*(2), 143-148.

de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*(1), 25-34.

Eloff, J. H., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, *12*(6), 597-603.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*(2-3), 203-225.

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, *256*, 57-73.

Freund, J., & Jones, J. (2015). *Measuring and managing information risk: A FAIR approach*. Oxford: Butterworth-Heinemann.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16-30.

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147-159.

Porter, M. (1981). The contributions of industrial organization to strategic management. *The Academy of Management Review, 6*(4), 609-620. Retrieved from http://www.jstor.org/stable/257639

Porter, M. E. (2008). *Competitive strategy: Techniques for analyzing industries and competitors*. New York: Simon and Schuster.

Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., De la Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, *39*(4), 774-784.

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information security and applications*, *18*(1), 45-52.

Sommestad, T., Ekstedt, M., & Johnson, P. (2010). A probabilistic relational model for security risk analysis. *Computers & security*, *29*(6), 659-679.

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), 45-56.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. Risk management guide for information technology systems.

Verendel, V. (2009, September). Quantified security is a weak hypothesis: A critical survey of results and assumptions. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 37-50). ACM.

Vorster, A., & Labuschagne, L. E. S. (2005, July). A framework for comparing different information security risk analysis methodologies. In *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 95-103). South African Institute for Computer Scientists and Information Technologists.

Wawrzyniak, D. (2006). Information security risk assessment model for risk management. In *Trust and Privacy in Digital Business* (pp. 21-30). Springer Berlin Heidelberg.

Yamin, S., Gunasekaran, A., & Mavondo, F. T. (1999). Relationship between generic strategies, competitive advantage and organizational performance: An empirical analysis. *Technovation*, *19*(8), 507-518.

## Review

This article was accepted under the ***constructive peer review*** option. For futher details, see the descriptions at:

http://mumabusinessreview.org/peer-review-options/

## Author

***Ed Fulford*** is is an executive in risk, information security, and compliance. He has more than 25 years of international experience assessing, building, and managing IT Security and Risk Management programs for companies such as CGI, CAPCO, RBS WorldPay, Fundtech Corporation, Cingular Wireless, and British Telecom. Fulford earned a Bachelor of Science in Business Administration from the University of Florida and a Master of Business Administration from Troy University. His professional certifications include the Payment Card Industry Professional, Certified Information Security Manager, Certified Information Systems Security Professional, Certified Fraud Examiner, and Certified Information Systems Auditor credentials.