Use Authorization

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at Idaho State University, I agree that the Library shall make it freely available for inspection. I further state that permission to download and/or print my thesis for scholarly purposes may be granted by the Dean of the Graduate School, Dean of my academic division, or by the University Librarian. It is understood that any copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Signature ______________________________

Date __________________________________

Visualizing Information Systems
Risk Model Usage Among
Professionals: An Analysis
# of Alternatives to ALE

by

Jeremy Brown

A thesis submitted in partial fulfillment

of the requirements for graduation with

Masters of Business Administration: Information Assurance Emphasis

from the College of Business

Idaho State University

April 2014

To the Graduate Faculty:

The members of the committee appointed to examine the thesis of Jeremy Brown find it satisfactory and recommend that it be accepted.

____

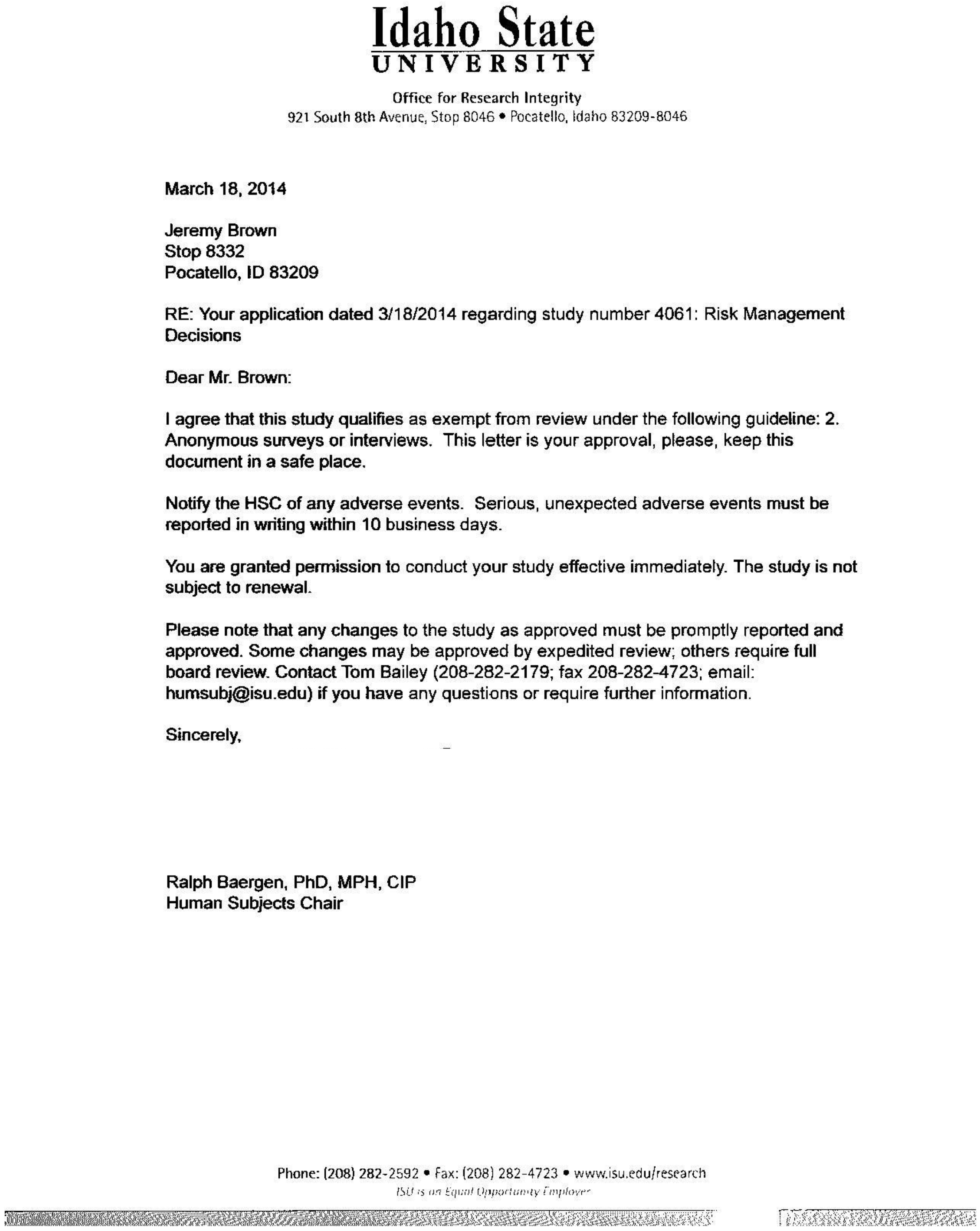
Dr. Corey Schou, Major Advisor

____

Dr. David Beard, Committee Member

____

Dr. Jonathan Lawson Graduate Faculty Representative



Idaho State
UNIVERSITY

Office for Research Integrity
921 South 8th Avenue, Stop 8046 • Pocatello, Idaho 83209-8046

March 18, 2014

Jeremy Brown
Stop 8332
Pocatello, ID 83209

RE: Your application dated 3/18/2014 regarding study number 4061: Risk Management Decisions

Dear Mr. Brown:

I agree that this study qualifies as exempt from review under the following guideline: 2. Anonymous surveys or interviews. This letter is your approval, please, keep this document in a safe place.

Notify the HSC of any adverse events. Serious, unexpected adverse events must be reported in writing within 10 business days.

You are granted permission to conduct your study effective immediately. The study is not subject to renewal.

Please note that any changes to the study as approved must be promptly reported and approved. Some changes may be approved by expedited review; others require full board review. Contact Tom Bailey (208-282-2179; fax 208-282-4723; email: humsubj@isu.edu) if you have any questions or require further information.

Sincerely,

Ralph Baergen, PhD, MPH, CIP
Human Subjects Chair

Table of Contents

Abstract vii

Chapter 1 - Introduction 1

1.1 - Introduction to the Problem 1

1.2 - Statement of the Problem 7

1.3 - Purpose of the Study 7

1.4 - Significance of the Study 8

1.5 - Assumptions 8

1.6 - Research Questions 9

1.7 - Operational Definitions 9

1.8 - Limitations 11

Chapter 2 – Literature Review 14

2.1 - Overview of Relevant Research 14

2.2 - Related or Theoretical Frameworks from Relevant Research 30

2.3 - Summary of Findings 36

Chapter 3 – Methodology 39

3.1- Design 39

3.1.1 - Overview of Study 39

3.1.2 - Research Questions 40

3.1.3 - Variables 40

3.1.4 - Research Method 41

3.2 - Description of Setting 42

3.3 - Sample 42

3.3.1 - Sampling Plan 44

3.3.2 - Human Subjects Protection 44

3.4 - Data Collection 44

3.4.1 - Method........ 44

3.4.2 - Instruments 45

3.4.3 - Reliability and Validity 45

3.4.4 – Procedure 47

3.5 - Proposed Statistical Analysis 50

Chapter 4 – Results 52

4.1 – Introduction 52

4.2 - Description of Sample 52

4.3 - Statistical Analysis 54

Chapter 5 – Discussion 59

5.1 - Summary of Major Findings 59

5.1.1 – Discussion 60

5.2 - Future Research 61

Appendix 63

References 65

Abstract

This study aims to test the assumption that Annualized Loss Expectancy (ALE) is the primary method of quantitative risk analysis used by a large subset of Information Assurance (IA) professionals. Results from an online cross-sectional survey support this hypothesis. By using the ALE method as a singular approach, and applying subjective opinions on the likelihood of impact and consequence, IA professionals are limiting the effectiveness of quantitative risk analysis. Several alternatives to ALE are available, providing unique approaches to quantifying information systems risk within the organization. The results of this research hold practical implications into the way that certified professionals handle the analysis of information systems risk, and illustrate that simplistic methods are not always the best choice for risk analysis.

Chapter 1 - Introduction

1.1 - Introduction to the Problem

Mankind has taken a keen desire to understand risk throughout history. Decisions like hunting, travelling, and warfare have posed great threats to human safety, and the concept of risk has followed us throughout these activities. Entire cultures were noted for their ability to perform risk analysis. Within the Tigris-Euphrates valley, a people called the Asipu lived around 3200 B.C. These early peoples served as risk consultants, who outlined and made decisions on the risk of several alternatives to a problem (Covello and Mumpower 1985). Society has found increased comfort in being able to define and choose alternatives in deciding what may happen in the future. This desire to predict future risk developed from a combination of fear and uncertainty (Bernstein 1996). By analyzing risk and reducing uncertainty, we have increased our own survival rates through history.

Bernstein notes the historical beginnings of quantitative risk analysis in the sport of gambling. Society became enthralled with the excitement of high reward payoffs, with little understanding of the risks involved. Human motivation to take risks by gambling is captured in Bernstein's quoting of Adam Smith, "The overweening conceit which the greater part of men have of their own abilities [and] their absurd presumption in their own good fortune" (1996). People who understood that gambling could be predicted with greater accuracy by quantifying the odds found a more consistent monetary reward, and continued to pursue a deeper understanding of risk.

Despite our affinity for gambling, very little was understood about numerical win/loss probabilities until a defined numerical system became available. This problem was solved in part by the work of Leonardo Pisano's (aka Fibonacci) publishing of *Liber Abaci*, also known as *Book of the Abacus* in 1202 A.D. This framework for substituting Greek, Hebrew, and Roman numerals for a scale of 0 to 9 on the Hindu-Arabic scale was revolutionary (Bernstein 1996). The flexibility of Fibonacci's work enabled historical discussions on probability; most notably captured in Pierre de Fermat's letter to Blaise Pascal (1654). These two concepts, in conjunction, provide foundation to the modern field of quantitative risk analysis.

For the purposes of this research, a widely available definition of risk will be used. The International Standards Organization (ISO) document 31000 defines risk as "the effect of uncertainty on objectives." Also important to note, the ISO defines effect as "a deviation from the expected – positive and/or negative" and that "uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood." This provides a solid base for understanding what risk means in modern times (International Standards Organization 2009).

Many different types of risk exist in today's society. Financial, healthcare, insurance, cybersecurity, and economic risk analysis are a small example of areas in risk management. Society has become enamored with the idea that risk can be completely eliminated; most likely because the reduction of uncertainty brings with it a level of comfort and assurance (Fischhoff, et al. 1981). Viewing risk as something that can be completely eliminated can cause a false sense of security. Risk will always exist; therefore, we must understand that risk management is less about eliminating risk and more about mitigating it to acceptable levels. According to Fischhoff et al., acceptable risk can be analyzed in the choice between alternatives (1981). This means that problems need to be examined and analyzed for the level of risk they inherently contain. Acceptable levels of risk involve examination of values, beliefs, and other factors which are organizationally defined. Once these have been established, the organization will have a clearer picture of what alternatives are acceptable to their risk management strategies.

However, this still leaves the daunting task of trying to quantify risk. This activity is often elusive because of the difficulty of quantifying uncertainty. Attempting to quantify risk also requires that the organization has knowledge beyond what is tangible; venturing into the valuation of intangible assets such as ideas, patents, information flows, and creativity. This is a problem because the value that one organization places on risk to intangible assets may be completely different than that of another organization. Therefore, applying a blanket approach to risk analysis can be dangerous to the organization. Different organizations require different approaches to risk management.

The field of Information Assurance (IA) is a continuously evolving discipline that is concerned with the protection and balance of five main information safeguards: confidentiality, integrity, availability, authentication, and non-repudiation (Maconachy, Schou and Ragsdale 2001). IA emphasizes the protection of these categories over time, which differs from the static method of Information Security (IS). Modern examples of IA groups that have shaped the foundation of

Information Systems Risk Management (ISRM), such as the Information Systems Audit and Control Association (ISACA) and International Information Systems Security Consortium (ISC^2), bring certification to the mainstream professional body. By increasing the professional certification levels through exams such as Certified Information Systems Security Professional (CISSP) and others, these organizations expose candidates to risk management strategies. These strategies include Business Impact Assessments, Disaster Recovery Plans, and Business Continuity Planning. Through the adoption of these techniques, security professionals become acquainted with the concept of both qualitative and quantitative risk.

The CISSP certification teaches a particular method of quantitative risk analysis, which traces back to the Federal Information Processing Standard (FIPS) Publication 65; a document which has since been replaced by the NIST SP 800-30. The formula was originally called Annual Loss Exposure, and intended for use in quantifying information systems risk. FIPS Publication 65 acknowledges the difficulty of obtaining exact monetary values for both impact and loss within the formula (United States Department of Commerce 1979). More recently, the formula is referred to as Annualized Loss Expectancy (ALE), and has been expanded into a more granular formula than its predecessor. More modern examples of information systems risk literature have included ALE as a primary method of quantitative risk analysis (Landoll 2006). The modern version of the formula is as follows:

ALE = Single Loss Expectancy (SLE) x Annual Rate of Occurrence (ARO)

SLE = Asset Value (AV) x Exposure Factor (EF)

Where AV = monetary value of the asset at the time of measurement, less depreciation.

EF = the impact of any given disaster, expressed as a probability ≤ 1

ARO = annual rate of occurrence, expressed as a probability ≤ 1

The output of ALE is expressed in monetary values, usually measured in U.S. Dollars. This formula enables the risk analyst to assign a yearly value to the amount of loss that each asset is expected to incur. By assigning this amount, the risk analyst can communicate the value of expected loss to management. From this point, managerment can make the decision as to how much spending will be allocated in mitigating the risks to the asset. Organizationally speaking, the value of risk mitigation should not exceed the loss expectation of ALE.

Since the ALE formula has gained acceptance as a method of quantitative risk analysis, and is taught to information security professionals who obtain certifications within the industry, there is reason to believe that it is frequently used to make decisions in ISRM. The ability to quickly determine the financial impact of risk, and appropriate levels of spending to handle that risk, is an important part of proactive ISRM decisions. In using ALE, the risk analyst has two decisions when determining values for EF and ARO. He may either assign these values by use of historical data – thus developing predictions based on statistical evaluation – or he may assign subjective probabilities based on his opinion of the likelihood of occurrence. The first option will take greater effort and expenditure of time, because the risk analyst must attempt to calculate the exact amounts needed for input into the formula.

For example, if an Information System Security Officer (ISSO) decides to estimate the EF and ARO for an internet-facing webserver that could be taken down by a power failure, he has the option to study past data on the reliability of the power grid. This requires both time and understanding of statistical methods of data analysis, such as regression or probability analysis. Taking this approach ensures that the results are more accurate; but the time and expense involved could be prohibitive. If the ISSO chooses the easier route – assigning subjective probabilities based on his opinion of likelihood – he is able to more quickly come up with a probability estimate at less expense. At this point he may as well be throwing numbers in, arbitrarily giving it his best guess, without the support that detailed research would provide. He has skipped objective analysis in the interest of efficiency. Although this gives him an “answer” much more quickly, the answer -- based on false data -- should not be relied upon for true risk analysis. This particular example outlines ALE’s acceptance of subjective analysis, as well as its limits in predicting the level of expected loss for risk mitigation spending.

In popular ISRM literature such as Federal Information Processing Standards (FIPS) Publication 199, International Standards Organization (ISO) 27005, and the National Institute of Standards and Technology (NIST) Special Publication 800-37, the categorization of systems by criticality level is a prerequisite to risk assessment. These systems are usually ranked in order of high, moderate, and low (National Institute of Standards and Technology 2004). Because different systems are bound to have varying levels of criticality, applying a blanket level of risk analysis on all systems may be harmful to the organization. If the risk analyst uses the ALE formula as a single way to evaluate loss potential, then systems of high criticality are subject to equally subjective risk treatment as systems with low criticality. This shows evidence of a problem, because high criticality systems may require more robust levels of spending to mitigate risk (Information Technology Laboratory 2010).

1.2 - Statement of the Problem

While the ALE formula may provide a simple method of quantifying information systems risk to high level management, it may be the primary method used within ISRM. By simplifying something as complex as quantitative risk analysis for IA, professionals may be inadequately assigning system risk, especially when framing that analysis with the use of subjective opinions to determine loss probabilities. The ALE formula provides IA professionals with an inadequate tool to quantify risk within organizational systems and networks. Using a potentially subjective approach to risk analysis limits the ability of the risk analyst to make accurate predictions, and gives management a false sense of security.

1.3 - Purpose of the Study

The purpose of this research is to visualize the realistic usage of the ALE model among ISRM professionals as compared to risk analysis methods. This will be done by analyzing results from an online survey, aimed at identifying which methods are actually used by certification-holding professionals in the ISRM field. By analyzing survey results, the assumption that ISRM professionals are using the ALE formula as a primary method of quantitative risk analysis will be tested.

Additionally, the literature review will outline relevant research and established frameworks within ISRM.

1.4 - Significance of the Study

The field of IA is vast and contains many different organizational types. By identifying trends within a subset of IA professionals, visualization of current IA risk management practices can be accomplished. This research can aid in identifying the gap between actual and assumed risk analysis methods. Organizations can use the recommendations within this research to begin the complicated task of finding the right risk management mix for their particular ISRM strategy. While this study is focused on ALE, its significance is greater than that, and should provide a helpful reminder that successful ISRM programs require both breadth and depth. There are no silver bullets within ISRM.

1.5 - Assumptions

When analyzing the efficacy of the ALE model, assumptions about the organization must be made. First, we must assume that the organization is aware and willing to take steps to analyze the risk to their information systems. Therefore, those organizations that simply ignore ISRM risk would not benefit from this research. Secondly, we must assume that organizations have assets which would benefit from risk identification procedures. If an organization doesn’t care about its assets, whether tangible or intangible, or the value therein, then research into risk analysis does little to benefit the organization. Thirdly, we must assume that threats to the organization, both external and internal, exist and possess the ability to take advantage of vulnerabilities within information systems. Should no threats exist to the organizations information systems or employees who operate them, then risk analysis would be a frivolous task.

1.6 - Research Questions

This research attempts to answer the following questions:

- Are career professionals within ISRM using the ALE formula as primary method of quantifying information systems risk?
- Are career professionals within ISRM using mathematical models (i.e. regression, probability analysis) as a primary method quantifying information systems risk?
- Are career professionals within ISRM using heuristics (previous risk decisions) as a primary method of quantifying information systems risk?
- Are career professionals within ISRM using best-guess assumptions as a primary method of quantifying information systems risk?
- Are there alternatives to the ALE formula for quantifying information systems risk?

1.7 - Operational Definitions

In order to understand their significance within this research, frequently used terms need to be defined by their use within IA. With the exception of the first term, which is an aggregate definition developed for this research, these definitions come from the glossary of NIST SP 800-30 (National Institute of Standards and Technology 2012):

- **Information Systems Risk Management (ISRM)** – the identification, assessment, and mitigation of risk associated with the operation and maintenance of information systems.
- **Confidentiality** – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity** – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Availability** – Ensuring timely and reliable access to and use of information.
- **Information Security (IS)** – Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.
- **Information Assurance (IA)** – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
- **Threat** – Any circumstance or even with the potential to adversely impact organizational operations, organizational assets, individuals, and other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

- **Vulnerability** – Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source.
- **Residual Risk** – Portion of risk remaining after security measures have been applied.
- **Risk Assessment** – The process of identifying, estimating, and prioritizing risk to organizational operations, organizational assets, individuals, and other organizations resulting from the operation of an information system.
- **Defense-in-Depth** – Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
- **Defense-in-Breadth** – A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every state of the system, network, or subcomponent life cycle.
- **Criticality** – A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function

1.8 - Limitations

Due to the nature of survey research, this study has limitations in the cross-section of IA professionals that it targets. The survey is aimed at a population of approximately 120,000 professionals who hold certification within the ISC^2 professional organization. This does not account for other IA professionals who belong to alternate certification bodies, or those who possess no certification at all.

Therefore, this research should not be taken as a representative study of the whole professional workforce within IA. Survey response rates provide additional limitations, with research showing average response rates for individuals at 52.7% with a standard deviation of 20.4% (Baruch and Holtom 2008). Given the relative time constraints of this study, a response rate of 1-3% would be considered successful.

For the sake of brevity and keeping participant response high, the survey does not include every single method of quantitative risk analysis. The survey asks about four options, which are statistical analysis, the ALE formula, best-guess opinions, and heuristics from previous risk decisions. This means that professionals who use other methods within ISRM to quantify risk are not accounted for. Since this survey is entirely voluntary, the results provided are from those professionals who are willing to take the time to provide feedback. Email distribution of the link to the online survey may also be caught up in the large volume of mail that the average person gets on a daily basis. Therefore, professionals who are not aware of the survey or unable to take the time to answer the questions are not represented in the results. The survey has launched quite recently, which also poses an additional limitation of time before graduation. Results of the survey should continue to improve in accuracy by the cutoff date of May 1st, 2014.

Literature review of risk management is robust, and provides plenty of approaches and frameworks to risk management from government, private sector, and academic sources. However, research into the history of ALE provides certain limitations; there is no clear link as to how the formula made its way from FIPS 65 to modern certification literature, which poses a limitation to understanding its history. Proposed methods of quantifying uncertainty are mathematically rigorous and intensive, such as non-gaussian ensembles in complex systems (Abramov and Majda 2004), and non-parametric estimators of probability (Ryan and Ryan 2006). These methods could be difficult to comprehend for risk analysts with limited knowledge of mathematics. The models themselves may serve as limitations when finding an alternative to the ALE formula.

Chapter 2 – Literature Review

2.1 - Overview of Relevant Research

As mentioned in the introduction, ALE found its roots in the FIPS Publication 65 with the caveat that exact numbers of impact and frequency of occurrence could "usually not be specified" (United States Department of Commerce 1979). The U.S. government realized early on that uncertainty would be difficult to quantify, and provided a method to estimate the cost of risk to information systems. Regardless of the acknowledged limitations, ALE is still a popular method of quantitative risk analysis, and is taught to information security professionals who obtain certifications within their career field (Gregg 2005). Many sources of research criticize the ALE model for incorporating subjectivity into the quantification of information systems risk. This is largely due to lack of empirical data on the frequency of occurrence of both impact and consequence, also known as the variables of EF and ARO within the formula (Mercuri 2003). In 1994, the U.S. government issued FIPS Publication 191, which again warned against the use of ALE as more than a preliminary risk evaluation tool. They advised agencies to analyze their own organizational needs for risk management in choosing which methods to use, suggesting alternatives such as automated risk analysis tools, and development of baseline security controls dependent on predefined levels of risk (National Institute of Standards and Technology 1994). During the 1994 publication, the U.S. government acknowledged the lack of any standard method of quantitative or qualitative risk analysis.

More modern examples of usage, such as Ali & Kap (2013), and Asosheh, Demoubed, & Khani (2009) show evidence that the ALE method can be used as a starting point for more robust forms of risk analysis.

In the first example, computer network vulnerability is modeled using a combination of host, vulnerability, attackers, and attacks. From here, probabilistic attack graphs are constructed to model a sequence of attacks against an information system, with respect to information dependencies between hosts. The ending output produces detailed probability analysis for the ARO portion of the ALE equation, leaving the system administrator to determine SLE values. By doing this, the ability to add subjective opinions about the likelihood of ARO is replaced by probabilistic analysis (Ali and Kap 2013).

The latter research shows an expansion of ALE in a different way. Traditional calculation of ALE is done to set a baseline, referred to as ALE1 or ALE before security controls are applied. Then security controls are applied, noting how much they will cost to implement. The second value, ALE2 is recalculated after applicable security controls have been implemented. Next, the ACC, which is the cost of implemented security controls, is figured. Following this, equation becomes (Asosheh, Dehmoubed and Khani 2009):

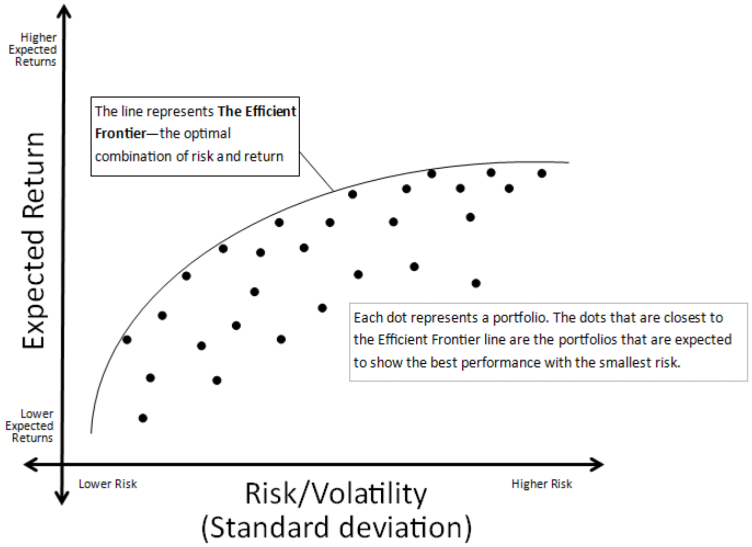
$$\boldsymbol{Return\ on\ Security\ Investment\ (ROSI) = ALE - ALE2 - ACC}$$

Both of the previous methods illustrate that ALE can be modified and used in creative ways to avoid subjectivity, at least in part. The first model nearly eliminates subjectivity, but is limited by the amount of time it may take to categorize and conduct probability analysis on hosts, vulnerabilities, threats, and attacks. The second model still facilitates the subjective assignment of both ARO and EF, but shows additional robustness in comparing ALE and security control costs. By calculating ROSI, the analyst can justify ISRM spending. If the ROSI is positive, then the controls implemented are cost effective at mitigating risk. This connection highlights similarities between cybersecurity and financial sectors because return on investment (ROI) is also used to evaluate the efficiency of investments in business (Investopedia 2014). If investments into risk mitigation are efficient, then the mitigation is a positive financial decision.

Boiled down to a simpler form, financial risk is the measure of the uncertainty of investments over time (Ahn and Falloon 1991). Risk affects financial decisions on a daily basis. In order to accurately understand financial risk, investors must learn to accept the inherent uncertainties within their financial portfolio and be willing to explore options for choosing the best risk/reward payoff. As outlined in the introduction of this paper, the concept of acceptable risk plays into financial analysis (Fischhoff, et al. 1981). If investors hold the belief that financial risk can be completely eliminated, they are mistaken.

Quantifying financial risk becomes a crucial piece in the investor's toolkit. A fundamental illustration of this concept is shown in the roots of portfolio theory. Dating back to 1952, with Markowitz's theory of Portfolio Selection, we begin to see the concept of reducing risk by way diversified investment choices. The efficient frontier graphically represents the best choice of investments with regard to expected return and standard deviation of portfolio returns (H. Markowitz 1952).

The following chart illustrates an example of the efficient frontier graph (Smart401k):

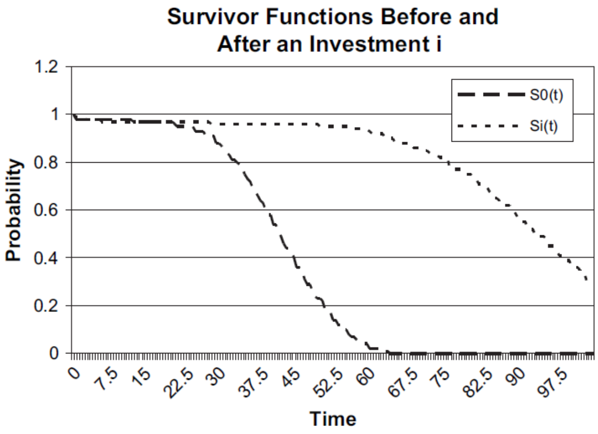


Markowitz's theory encourages the right kind of diversification for the right reasons, as well as portfolio building with investments that have low co-variance; a term referring to the strength of correlation between two variables. Usually, this means choosing investments from within different sectors (i.e. medical and financial). By investing in securities with low co-variance, the overall riskiness of the portfolio decreases in comparison to a singular investing strategy. As research points out, the strategy of portfolio diversification is dependent on both the return expectations of the investor, and the value they place on having stable and/or dependable returns. Later on in his work on portfolio selection, Markowitz points out that investments with the lowest standard deviations do not necessarily possesses the lowest expected returns (H. M. Markowitz 1959).

While the financial sector largely removed from the modern field of IA, we can apply concepts from portfolio theory and financial risk diversification to that of ISRM. This concept was touched upon in earlier IS literature, with the largely qualitative portfolio approach to information systems (McFarlan 1983). To establish the basis of this theory, we must assume that securities within the financial market hold similarities to risk management approaches. That is to say, that having only one way to quantify risk to the organization, like ALE, may be similar to choosing only one security based off of its expected return. Including several risk management strategies within a portfolio decreases the risk of total failure. If one strategy fails to quantify risk and provide alternatives, then others in the portfolio can provide redundancy. This also implies that radically different methods of risk analysis (sectors) be chosen for the portfolio. By applying Markowitz's theory of portfolio selection, we can start to see the value of developing efficient risk management portfolios within ISRM.

In strengthening the connection between portfolio theory and ISRM, we need to examine two very fundamental aspects of IA: defense-in-depth and defense-in-breadth. Defense-in-depth places layers of heterogeneous obstacles between ISRM threats and vulnerabilities, while defense-in-breadth focuses on a wide variety of different defensive postures. The combination of both creates both defensive power, and redundancy, with the only downfall being increased ISRM costs (Cleghorn 2013). Based on the needs of the organization, a portfolio of risk management strategies could be created to mimic a defense-in-depth (or defense-in-breadth) approach; eliminating reliance on just one form of risk analysis. From this point, organizations could analyze which risk analysis methods provide the lowest acceptable risk.

ISRM investment requires careful analysis by management in both IA and financial decision committees. Research shows that risk can be quantified in a much more accurate way than assigning subjective probabilities, such as calculation of expected loss within the information system (Ryan and Ryan 2006). This calculation takes into account the loss function, or the amount of loss that we would experience if a successful attack were to take place within the infrastructure. This is a function over time. Survivor curves are calculated on the basis of Kaplan-Meier estimators, which show that the probability of system survival decreases over time. This illustrates that information security is never perfect, and systems will eventually fall to attacks. The following graph illustrates the survivor function moving to the right, a goal of effective risk spending (Ryan and Ryan 2006):



The research shows that not all information investments are wise. The only investments that should be made are those that move the survivor curve to the right, or to a point which may outlast the attack duration. ISRM funding decisions should, therefore, be measured by the amount of survivability (or security) that they add to the system – which shows the inverse of risk. As security increases through investment, risk will inversely decrease (Ryan and Ryan 2006). However, certain investments may provide little to no survivor curve movement, illustrating either diminishing or non-realized returns.

Providing accurate methods to calculate risk spending is a notoriously difficult task (Ryan and Ryan 2006). Where many risk frameworks, such as NIST 800-30, CORAS, and ISO 27001, view risk as a crossroads between threat likelihood and threat impact, Ryan's research describes risk as the inverse of security. In this way, measuring the increases to security, quantifies reduction in risk. Traditional methods, such as the ALE formula have not approached risk analysis in this way. Spending through ALE does not directly relate to quantifiable increases in information security. With this knowledge, the improper use of ALE can cause a false sense of security from ISRM spending.

Other innovative solutions to quantitative risk analysis have been developed among ISRM literature. Conflicting Incentives Risk Analysis (CIRA), developed by Rajbhandari & Snekkenes, shows the crossroads of combining ideas from game theory, economics, psychology, and decision theory into risk analysis (2012). In CIRA, the risk analyst switches subjective probability analysis for "stakeholder perceived incentives," which provide a more easy set of inputs to audit when performing risk analysis. This paper argues that subjective risk decisions break down when little to no data exists to validate probability or rate claims (Rajbhandari and Snekkenes 2012).

CIRA's approach substitutes traditional risk probability assignment for stakeholder incentives; that is, decisions that provide positive value to either the strategy owner or the risk owner. These utility factors are decided based on survey results given to both risk owners and strategy owners. The example used to illustrate this is the Social Networking Service (SNS) model. The risk owner is the user who depends on the SNS to communicate with the world, and the strategy owner is the provider of the SNS, turning availability and customer service into profit. Incentive is computed as change in utility (both negative and positive). The example shows risk owner (SNS customer) as having two utility factors; privacy and satisfaction (availability, support, and service completeness), while the strategy owner (SNS provider) values profit and privacy reputation. In order for either component to make a first move, or introduce a different level of risk into the game, then the incentive to change one's own utility factor must be stronger than that of the loss to other utilities and other players. This reframes the risk question from "How often will the event occur?" to "What benefit does a player seek to benefit from the incident? (Rajbhandari and Snekkenes 2012)"

CIRA is a completely different approach versus traditional methods, such as ALE. When using a traditional implementation of ALE in risk analysis, shareholders are not taken into account. The CIRA method may provide a viable alternative when data is lacking for probability analysis, or when new risk territory is being explored.

The idea of viewing risk from a systemic perspective is adopted by several frameworks, such as NIST 800-30 and ISO 27001. As one component of a system changes, the potential to place other data sources at risk may change drastically.

Traditional risk management models, both quantitative and qualitative, are mostly static methods of evaluation (Lei 2012). As Lei argues, the changing of system components will change the security properties of the system as a whole. Thus, a model of risk evaluation was developed, incorporating the dynamic elements of real-world business change within the information system. This model, referred to as the Dynamic Risk Evaluation Model, sets out to accomplish a synchronicity between change management and risk analysis. The model demonstrates the transformation from network map to topological and component structures. This process is illustrated in the following graphic (Lei 2012):

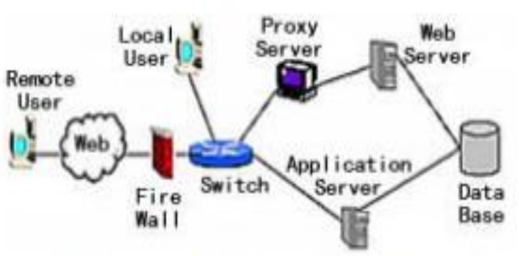


Figure 1. A reality application information system

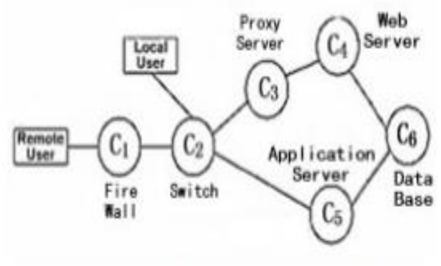


Figure 2. Topology structure of information system

Once the topological diagram has been established, then “visiting routes” can be formalized. A route is defined as the path a user may take from any point on the edge of the system. To perform a task, the user will establish various visiting routes, and if these are down, it is considered a failure in system security (Lei 2012). Visiting routes that establish connection with externally viewable machines, such as the proxy server or public web server, present a level of risk that is higher than internally protected systems. When a visiting route is operating correctly, the systems that are contained within it have a collaborative relationship (Lei 2012). If this collaboration breaks within the user’s session, or is denied from taking place by an outside party, the user faces risk in not being able to complete the task at hand. Also important to the model, is the layout of the systems, which are either parallel or serial. Very serious risk can occur in a serial connection, because a single point of failure can be identified. Parallel systems may be more lenient in route operation, due to the failover inherent with their design. In the model, systems are assigned a security value of either 1 (most secure) or 0 (least secure). Utilizing a broad approach, risk can be analyzed by the summation of security values within the system (Lei 2012).

Dynamic changes to the system-wide risk profile can occur in three ways:

1. The Security Property of A Certain Component Changes
2. Increasing the Components Within the System
3. Reevaluation After A Dramatic Change

Lei's research provides an example of adding a firewall to the system. This requires increasing the number of components in the system, and the reevaluation of all components that would collaborate with the new component; changing the overall risk profile of the system. This method of analysis is expected for all new additions to the information system. NIST 800-37's guide to the Risk Management Framework also takes a similar view. Step 6 of the RMF, the monitoring of information security controls; outlines the need for risk reevaluation when system components are replaced or upgraded (Information Technology Laboratory 2010). Both Lei and NIST 800-37 emphasize the importance of system wide analysis and the impact of each component in collaboration. Dynamic risk analysis may be a fundamentally stronger approach to identifying security concerns. Static models such as ALE may be doing harm to systems that require reevaluation of components based upon their interaction and the specific purpose that they serve within the infrastructure. Statically evaluating risk places emphasis on risk in the present instead risk in the future. This is dangerous to the organization because it does not take a proactive approach to risk analysis. Dynamic models, due to their continuous nature, can provide more timely and accurate data for spending decisions.

Research has found uses for expert opinion within risk management. The field of ISRM can also benefit from borrowed knowledge within non-related academic fields, such as genetics. Within this field, creative approaches such as the Genetic Algorithm (GA) analysis based on natural selection, have surfaced as alternatives to the ALE formula.

This research uses GA's developed by Johan Holland and colleagues at the University of Michigan. The purpose of these GA's is twofold: to thoroughly explain the adaptive processes within natural systems, and to design artificial software systems that learn adaptive processes in natural and artificial systems (Tamijidyamcholo and Al-Dabbagh 2012). These GA's quantitatively process current generations of creatures and produce outputs of the fittest offspring that are possible from any given set of species. This information utilizes historical data to speculate on future generations, with the goal of creating offspring with a higher probability of survival. By ensuring the fittest parts of previous generations are allowed to pass through, the risk of extinction is minimized within the genetic sequence and should theoretically diminish over each subsequent generation. This process is split into six steps:

1. **Initialize GA Variables**
2. **Generate Initial Generation**
3. **Evaluate Fitness Function for each Chromosome**
4. **Selection Operation**
5. **Crossover Operation**
6. **Mutation Operation**

Much like the Risk Management Framework outlined in the NIST SP 800-37 document, the GA implementation of risk analysis starts out with asset categorization (Information Technology Laboratory 2010). Tamijidyamcholo & Al-Dabbagh's model takes the approach of delivering surveys to subject matter experts. These surveys are relevant in identifying the GA variables. Within the model, these variables are:

- **VA** – Information Asset Value (1 to 100)
- **LV** – Probabilistic likelihood of vulnerability occurrence (0 to 1)
- **MC** – Percentage of risk mitigated by current controls (0 to 100%)
- **UV** – Percentage of uncertainty in current knowledge of vulnerability (0 to 100%)

Forming the equation:

$$\boldsymbol{Risk\ Rate} = \boldsymbol{VA} \times \boldsymbol{LV} - (\boldsymbol{VA} \times \boldsymbol{LV}) \times \boldsymbol{MC} + (\boldsymbol{VA} \times \boldsymbol{LV}) \times \boldsymbol{UV}$$

These variables come together to form the Risk Rate, a value that is either acceptable or not. If the Risk Rate is higher than defined organization risk limits, the GA is run on the variables within Risk Rate to determine which variables stand the smallest chance of propagating to the next generation. Those variables that have the weakest impact on overall system risk are subject to analysis by risk mitigation experts (Tamijidyamcholo and Al-Dabbagh 2012). Over the process of calculation, weak variables are exposed and subject to change until a risk level is equal to or lesser than organizationally defined risk minimums. Should management decide to leave the risk level at higher levels than the organization mandates, they must go through the process of risk acceptance.

Although the GA research offers a unique approach to risk minimization, it may still suffer from the same basic problems that plague the ALE formula. The last three variables of LV, MC, and UV are all based on the subject matter expert's opinion on outcomes. The research also states that the goal of the GA is to reduce risk level to 0 (Tamijidyamcholo and Al-Dabbagh 2012). Research has indicated that no measure of security is perfect; suggesting that increasing the time it takes for a system to succumb to attacks is a more effective method of risk mitigation (Ryan and Ryan 2006). Additional limitations to this research include the example GA analysis being run with a singular vulnerability, threat, uncertainty, and information asset identified. While this provides a simple proof of concept, it does not reflect realistic IA practices within many organizations, because information systems risk cannot be completely eliminated, and most organizations have more than one asset to protect at any given time.

Risk can be viewed in a multitude of ways, from whole systems to individual components. This provides a wide range of risk analysis, based on organizationally defined policies. Using narrow approaches to risk management (i.e. the ALE formula); as the primary decision method increases the chance of inaccurate analysis within ISRM. Combining previous work the field of ISRM, the following article explains a multi-pronged risk metric called Perceived Composite Risk (PCR). Bodin, Gordon & Loeb explain PCR as a metric that takes into account three common risk decision criteria (2008):

- Expected Loss (EL)(equivalent to ALE) – E[X]
- Expected Severe Loss (ESL) – $E[X|X \geq T]$
- Standard Deviation of Loss – σ

The authors of the article recommend a unique approach to the problem of assigning probability to both the EL and ESL categories, which is the use of the Analytic Hierarchy Process (AHP) (Saaty 1987). This process develops a theory of measurement which is unique to the analytical needs of the observer. In this specific example, weights are drawn based on priorities outlined by the Chief Information Security Officer (CISO) as to the importance of each asset to the business. To eliminate the subjectivity of his own opinion, the CISO can survey his employees for suggestions as to the importance of each asset.

The value of the PCR approach is shown in the variety of inputs that are used to calculate the risk model. As compared to a singular approach like ALE, the PCR model uses three distinct measurements. While the first prong of PCR is essentially the ALE formula, the use of both ESL and standard deviation of loss; take the focus off of the subjectivity that ALE allows. The authors argue that the use of PCR aids in the actual decision process of budgeting risk mitigation of assets (both tangible and intangible) within information systems (Bodin, Gordon and Loeb 2005). Within the PCR model, the weight of ALE within the model is reduced. Therefore, the ability to assign subjective opinions on likelihood is reduced as compared to using a singular approach like the ALE formula.

By now, the ability to assign subjective opinions to likelihood of occurrence with ALE has been outlined by research. The problem of deciding accurate and organizationally specific information risk probabilities is recognized as a difficult task. Several unique attempts, such as Wavelet Neural Networks (WNN) have been proposed to find a solution to the problem (Chen and Zhao 2013). This radically different approach uses WNN as a basis for machine learning to take place. In turn, this model attempts to quantify risk to information systems.

Machine learning is a useful subset of artificial intelligence in which algorithms are utilized to transform large data inputs into predictable and repeatable outputs. As data is absorbed by the system, the system "learns" how to deal with data more effectively. Early research by J.R. Quinlan into decision tree analysis has lent a great deal of foundational knowledge in the field of machine learning. In particular, decision trees are efficient at dealing with incomplete data fields or those that possess incorrect information (Quinlan 1986). Since organizational risk analysis often deals with incomplete and/or subjective decisions, this approach may be useful in dealing with the noise that comes with risk analysis data.

Since WNN's fall within the subset neural of networks in the hierarchy of machine learning, we can further understand the usefulness of the method within ISRM. WNN's give researchers the ability to process the complicated learning of non-parametric functions (Zhang, et al. 1995). Since risk data does not typically deal with statistical means, standard deviations, or variances, WNNs may be an effective way to learn risk functions.

In Chang & Zhao's research, the WNN is aimed at reducing the error rate between expert risk analyst decisions (taken via risk survey) and machine learning algorithms that accomplish the same task: to evaluate an information security risk model based on the following five categories (Chen and Zhao 2013):

- Information Security Risk Vulnerabilities
- Threats
- Capability Loss
- Asset Loss
- System Recovery Cost

These categories are setup in a decision tree format; assigning weights to each branch based on fuzzy evaluation. The model shows proof of concept that machine learning can produce similar results to a panel of experts at a maximum of 5% error, with the average being 2.86%. A panel of 200 professionals is used to illustrate that the WNN method is successful in learning the factors that assign accurate levels of risk to each of the aforementioned categories at an error rate that is less than expert recommendation (Chen and Zhao 2013). Thus, machine learning may have the ability to carry out risk analysis with greater accuracy than a team of experts who rely on subjective opinions or career based experience to determine likelihood.

2.2 - Related or Theoretical Frameworks from Relevant Research

A commonly accepted private sector standard for information systems risk is the International Standards Organization (ISO) 27005 document. It provides a framework for ISRM and references the previous work of ISO 27001 – 27002 as helpful precursor documents. Defining risk estimation as the "process to assign values to the probability and consequences of a risk," this document lends itself to the subjectivity of opinions in the ALE formula. Since ISO 27005 is a guideline, it shows no preference between objective and subjective risk analysis. This document, like others in the field, explains risk in the context of likelihood and consequences, which are equivalent to EF and ARO within the ALE formula. These can be used to assign a dollar amount to risk.

ISO 27005 outlines that risk treatments for ISRM must be prioritized. The goal of prioritizing the ISRM within the organization should be to reduce the overall amount of residual risk after all categories have been assessed. Use of this framework provides alternatives for dealing with risk to the organization. These categories of risk treatment are (International Standards Organization 2008):

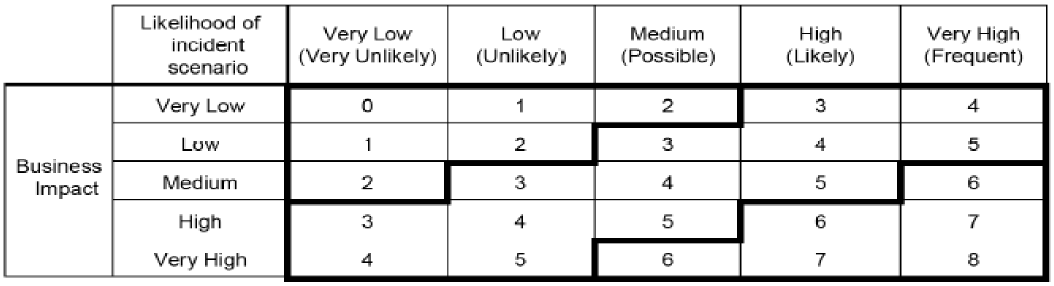
- **Risk Reduction** – Identifying security controls which reduce risk to a level which provides acceptable residual risks.
- **Risk Retention** – Special situations in which investment into reducing risk is more costly than simply accepting the risk.
- **Risk Avoidance** – Withdrawing from activities or projects which introduce higher levels of risk then are organizationally acceptable.

- **Risk Transfer –** Transferring risk to parties that are more adequately equipped to deal with it.

Before these risk treatments can be applied, identification of system boundaries and system risk assessment must be conducted. During the assessment phase, the identification of primary assets takes place. ISO 27005 views assets as anything of value to the organization and which requires protection. This model places assets under one of two categories: business processes and activities, or information. Once assets have been identified, they must undergo valuation (International Standards Organization 2008).

While many assets have a specific monetary value, all others are defined on an organizationally developed scale, usually ranging from very high to very low criticality. For example, the valuation of an intangible asset, such as patents or employee ideas, would be difficult to quantify objectively. Many organizations value these assets on a subjective scale, gathering the opinions of multiple stakeholders. If organizations can successfully implement an objective financial valuation of these categories, then the model becomes stronger. Additionally, ISO 27005 provides the flexibility to factor in the loss of confidentiality, integrity, availability, authentication, and non-repudiation.

The crossroads between impact and likelihood provides risk prioritization within ISO 27005. As the following table shows, an organization should invest higher amounts of money into mitigation and security control selection as likelihood of occurrence and/or business impact increases (International Standards Organization 2008):

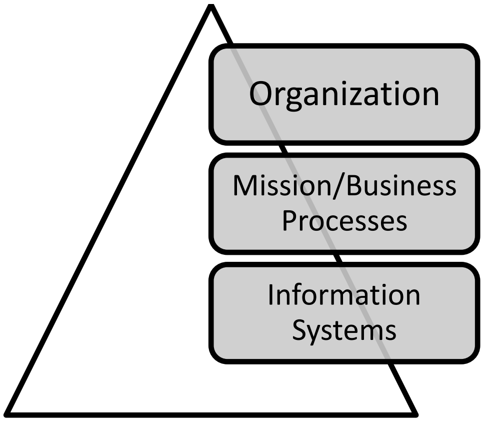


	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

ISO 27005 also offers the flexibility to choose either qualitative or quantitative risk valuation methods for assets. As such, the ALE formula can be used within ISO 27005 to quantify risk to information systems. As previously mentioned, ALE is an easier way to make recommendations about risk mitigation spending to management. By using ALE, organizations must realize and accept the residual risk of subjective opinions in determining likelihood. Divisions who need additional funding may suffer from bias about their own levels of risk. This is dangerous, because lack of objectivity can lead to inaccurate risk analysis and lack of protection for valuable assets that may be compromised.

The National Institute of Standards and Technology (NIST) have released several helpful documents within the IA career field. More specifically, the document that deals with ISRM is referred to as Special Publication (SP) 800-30. This document, along with other NIST SPs, establishes guidelines for compliance with Federal Information Security Management Act (FISMA), in operation of systems and networks owned by the United States Government, and those contracting organizations who act on its behalf (National Institute of Standards and Technology 2012).

Much like ISO 27005, NIST SP 800-30 views risk as a combination of impact and likelihood. The framework provides guidance in identifying relevant threats, vulnerabilities, impact of threats, and likelihood of harm. To illustrate this framework, a three-tiered approach is used (National Institute of Standards and Technology 2012):



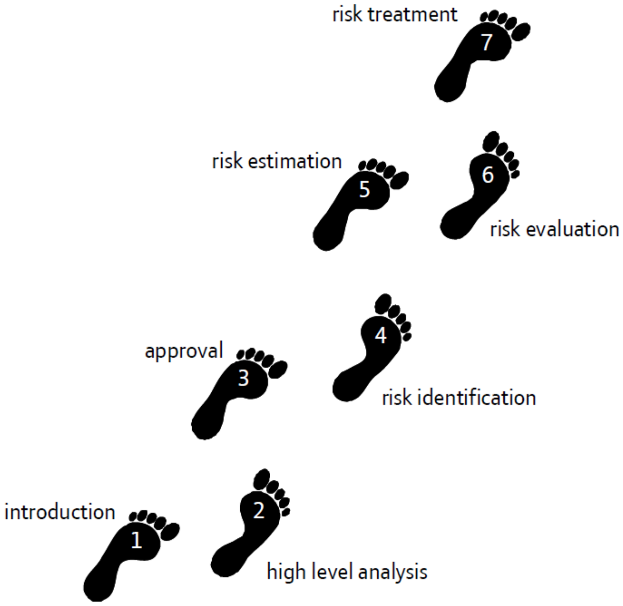
Risk assessments within NIST 800-30 may be conducted on all three tiers, but each has its own specific use-case. From an ISRM perspective, the individual who is analyzing threats to an organization has a fundamentally different duty than his counterpart who is focused on information systems. Government agencies may consider the Advanced Persistent Threat (APT) – a series of carefully managed and organized attacks performed by nation-state actors – to be an example of risk against the organization. Threat sources like APT do not present as significant of threat to daily operations. Thus, quantifying risk within NIST 800-30 depends on the task at hand.

Much like ISO 27001, NIST SP 800-30 can accept quantitative risk models, such as the ALE formula. The publication notes that the rigor of the quantitative model reduces inversely to the amount of subjectivity, or subjective human risk decisions that are included in risk analysis. For example, NIST SP 800-30 would support the subjective opinion that an earthquake may hit datacenters in Alaska with a .04% annual likelihood; but without historical data or statistical analysis to back this claim up, the rigor of the model may provide inadequate advice on risk mitigation spending.

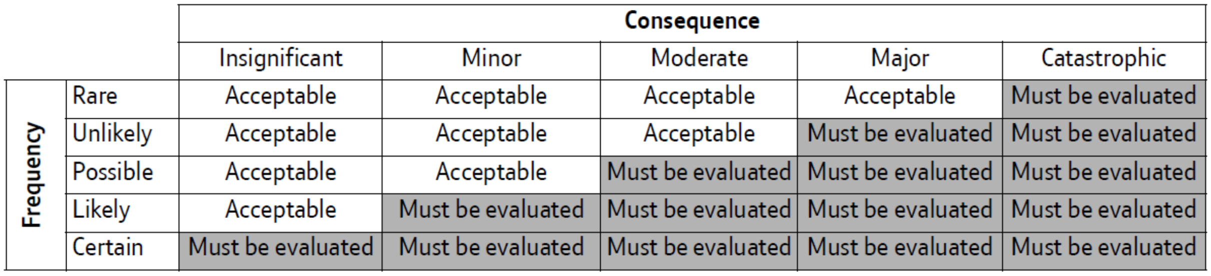
Entering into the field of model based risk analysis; we are presented with the CORAS method. Developed by a conglomerate of 3 commercial companies, 7 research institutes, and 1 university, this is a Universal Modelling Language (UML) based tool that aims to develop a “precise, unambiguous, and efficient risk analysis” platform (Gran 2002). CORAS is a software tool hosted on SourceForge, which provides users a way to create diagrams according to the layout of their information systems. CORAS aims to answer questions through its modeling techniques. The typical organization who is interested in the CORAS method would start with simple inquiries such as:

- How safe is my online customer database?
- Should I worry about identity theft when using a work computer for shopping?
- What are the impacts of one single incident of insider espionage to my company?

Once questions have been raised, then a framework of seven steps is followed to track the progress of risk analysts in respect to the organization. The following diagram is directly taken from the CORAS documentation (Braber, et al. 2007):



For the sake of brevity and lack of relevance to this research, the seven steps of CORAS will not be explained in depth in this literature review. However, the first four steps can be effectively summarized in the relationship and communication between the risk analyst and client(s). The last three steps heavily involve the client and make use of workshops to identify and estimate risks to the modeled target scenario. Of particular relevance to this research is step 5, which focuses on risk identification and estimating the likelihood (or probability) of each threat occurrence. Within step 5, this model welcomes quantitative analysis, such as the ALE formula. In similar fashion to both NIST SP 800-30 and ISO 27005, the CORAS method establishes a risk matrix as a general guideline (Braber, et al. 2007):



		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare	Acceptable	Acceptable	Acceptable	Acceptable	Must be evaluated
	Unlikely	Acceptable	Acceptable	Acceptable	Must be evaluated	Must be evaluated
	Possible	Acceptable	Acceptable	Must be evaluated	Must be evaluated	Must be evaluated
	Likely	Acceptable	Must be evaluated	Must be evaluated	Must be evaluated	Must be evaluated
	Certain	Must be evaluated	Must be evaluated	Must be evaluated	Must be evaluated	Must be evaluated

While following this matrix is at the discretion of the organization, it provides a starting point to visualize risk with UML modeling. Boxes that require evaluation are subject to workgroup collaboration between the risk analyst and client(s), which is highly dependent on the amount of interaction between the two parties (Hogganvik and Stolen 2006). Determining factors such as impact and consequence in step 5 can be accomplished and translated easily from analyst to client by using the ALE formula. Because ALE has obvious vulnerabilities in determining subjective likelihood, using this method within CORAS may lead to inaccurate risk estimation by the analyst. If a client doesn't truly understand the analysis behind the risk estimation process, then a false sense of security can occur. Knowing this, clients are ill-equipped to determine ISRM budgets.

2.3 - Summary of Findings

Examining the history of the ALE formula shows that it was developed as a simple way to estimate the levels of impact and likelihood when quantifying risk (United States Department of Commerce 1979). The output of ALE provides analysts with a method of monetizing information systems loss. This method came with limitations, which primarily dealt with the ability of the analyst to apply subjective opinions in the areas of impact and likelihood. This exposed the model to criticism of accuracy in determining true expected losses. Expanding upon the work of FIPS 65, FIPS 191 further explained the limitations of using ALE, even recommending qualitative methods of risk analysis as alternatives to the formula (National Institute of Standards and Technology 1994). Despite the stated limitations, the ALE model has continued to propagate into modern ISRM research and industrial certification literature as an acceptable method of quantitative risk analysis.

Given the prevalence of the ALE model, researchers have developed models to minimize the level of subjective inputs to the formula (Ali and Kap 2013) and (Asosheh, Dehmoubed and Khani 2009). These approaches provide a unique method of adding robust feature sets to the basic ALE formula. Rather than propose alternatives, they emphasize rigorous determination of probability, and return on investment principles from the field of finance, respectively.

Similarities can be drawn between IA and financial risk career fields, specifically in generating a theoretical approach to security portfolio development. This synthesizes the early work of Portfolio Selection by Markowitz (1952) with McFarlan's theory of information systems portfolios. There are similarities between risk approaches and investments within portfolios. Organizations behave similar to individuals in that they seek risk management approaches with greater expected returns and less risk. If we assume that organizations are behaving this way, than we can see the benefit of creating efficient portfolios of risk management methods, which should be radically different from each other. The idea of varying risk methods begins to look similar to the IA concepts of defense-in-depth, and defense-in-breadth (Cleghorn 2013). Using strategies within a portfolio that focus on removing subjectivity from the ALE model illustrates defense-in-depth, while implementing radically different risk management methods, such as CIRA

(Rajbhandari and Snekkenes 2012), PCR (Bodin, Gordon and Loeb 2008), and Ryan's expected loss function (Ryan and Ryan 2006) illustrates defense-in-breadth.

Making the connection between IA and finance concepts shows that risk analysis can be approached from new and creative ways, employing crossover knowledge from research in other fields. Creativity in risk analysis prevents stagnant approaches to evolving problems. Both GA risk analysis (Tamijidyamcholo and Al-Dabbagh 2012) and WNN machine learning methods (Chen and Zhao 2013), provide crossover from completely different career fields than IA. Both unique risk assessment models provide alternative approaches to the ALE formula.

The synthesis of literature in this research shows obvious flaws in ALE: if risk analysts choose to include their subjective opinions about the occurrence of impact or likelihood. Given this statement, the literature outlines several viable alternatives to ALE. These alternatives range from reducing subjectivity in the ALE model, to models that are derived from knowledge in the career fields of finance, biology, and computer science. By understanding some of the alternatives to ALE, organizations can develop more robust approaches to risk management. This provides them with choices in determining organizationally-defined acceptable risk.

This literature review enriches the purpose of the study. Visualizing the most common risk analysis approaches within IA professionals will help to bring forth the preferred method. If this method confirms the hypothesis of ALE over-use, then alternatives can be suggested to mitigate this problem among IS professionals. This adds robustness to the risk analysis process, which benefits the goal of ISRM.

Chapter 3 – Methodology

3.1- Design

3.1.1 - Overview of Study

The purpose of this research is to examine and visualize the realistic usage patterns of the ALE quantitative risk analysis formula among information security professionals, as compared to statistical analysis, best-guess, and heuristic methods of risk analysis. The method of collecting this information will be through a cross-sectional online survey sent to a group of IA professionals. Additionally, this survey collects data on the estimated annual budget for ISRM spending, and years of management that professionals have at the time of taking the survey. Collected information will help provide a look into a specific subset of IA professionals from ISC^2, in regards to which quantitative risk methods are used in their analyses.

Motivation for this study came from taking the CISSP and SSCP exams and noticing that nearly all quantitative risk was taught in the form of the ALE formula, and implying that ALE is the only method used by professionals who also possess certifications within the IA career field. The results of this research will test the validity of this implication for the specified survey population.

The organization of this chapter will provide background into the research methodology and questions. Variables are defined within the context of this research as well as a description of the setting and research methods used to the conduct study. It is important to note that this study has exempted status from the Idaho State University Human Subjects Committee, due to the use of anonymous survey results.

3.1.2 - Research Questions

Included in the appendix is the 7 question information systems survey distributed to members of ISC^2. This survey gathers results aimed at answering two research questions, while the review of relevant research within the ISRM field provides the final question for analysis:

1. Among the surveyed population, is usage of the ALE quantitative risk analysis formula greater than that of statistical methods, best-guess analysis, or heuristics?
2. Do years of management experience within the IA or IS field correlate with the yearly estimate of annual spending on ISRM?
3. Are there alternative methods to ALE for quantifying information systems risk?

3.1.3 - Variables

Questions within the survey are aimed at identifying a preference between four different methods of risk analysis among IA professionals. These trends are explained by the following variables:

- ALE – Participant determines quantitative risk to information systems using the ALE formula. This variable prompts a yes/no response which can be coded into binary values (0,1).

- STAT – Participant determines quantitative risk to information systems using statistical methods, such as regression. This variable prompts a yes/no response which can be coded into binary values (0,1).
- HEUR – Participant determines quantitative risk to information systems using heuristics (quick solutions) from previous risk decisions. This variable prompts a yes/no response which can be coded into binary values (0,1).
- BG – Participant determines quantitative risk to information systems using a best-guess from previous career experience. This variable prompts a yes/no response which can be coded into binary values (0,1).
- RSKMGT – Participant has been tasked with the risk management of information systems to include risk analysis, risk mitigation, risk transference, or risk acceptance. This variable prompts a yes/no response which can be coded into binary values (0,1).

3.1.4 - Research Method

The selected research methodology consists of an online, cross-sectional survey to be distributed to members of ISC^2, for the purposes of gathering information about professional usage of risk analysis methods. This information will help to identify the predominant risk approach that is used among the surveyed participants. By analyzing survey results, the frequency of ALE usage will be discovered.

3.2 - Description of Setting

The entirety of the study will be held in an online survey setting, with questions administered through the SurveyMonkey website. This provides participants the choice of where they want to take the survey. This survey is completely anonymous, as outlined by the Human Subjects Committee at Idaho State University. Participants are informed before the start of the survey that their participation is voluntary. They also have the option to quit taking the survey at any time. This provides less participant pressure than a traditional pen and paper survey that is administered in a formal setting.

The reason for selecting the online setting for the study was to provide maximum flexibility and outreach to the audience, of 120,000 members of ISC^2. The resources that would be required to distribute a survey of this magnitude to participants via direct mail or paper copy would be immense; far beyond personal resources and time constraints. While the online survey setting may provide flexibility, it also reduces participant accountability for actually finishing the survey as compared to proctored methods, such as direct survey administration. The large population that becomes available via ISC^2 mailing list should make up for any lack of participants who do not fully complete the survey.

3.3 - Sample

The survey is targeted at 120,000 members of the professional cyber association of ISC^2. This population was selected because of membership within a professional association, which increases the likelihood of reaching an audience that has experience with ISRM. Due to time constraints, this survey will not reach other professional organizations within IA, except for those members of ISC^2 that hold membership in other organizations. For proof of concept, the existing membership of participants will suffice.

Participants were chosen based on the membership criteria of ISC^2. To be a member in good standing with this organization, you must hold at least one professional certification from the following list:

- Systems Security Certified Practitioner (SSCP)
- Certified Information Systems Security Professional (CISSP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Cyber Forensics Professional (CCFP)
- Healthcare Information Security and Privacy Practitioner (HCISSP)

In addition to holding one or more ISC^2 certifications, members must remain in good standing with the organization. This requires three steps (International Information Systems Security Certification Consortium 2014):

- Abide by the ISC^2 code of ethics
- Submit annual maintenance fees (AMFs)
- Obtain and submit the required continuing professional education (CPE) credits as required by each certification

By making members accountable for gaining CPEs, the organization keeps a level of professional knowledge within its membership ranks. This also keeps members up to date on security knowledge within the IA and IS field. Members who are joining ISC^2 or obtaining additional certification within the organization must be sponsored by fully certified members within. This provides a two-factor system of integrity in membership decisions. This validates the integrity of survey audience.

3.3.1 - Sampling Plan

For the purposes of this research, no sampling plan will be used. The analysis of data will aim to visualize the responses of the survey participants, rather than performing advanced statistical analysis. Simple statistical analysis, such as descriptive statistics and correlation will also be performed on survey responses.

3.3.2 - Human Subjects Protection

The Human Subjects Committee at Idaho State University has granted this study exempt status for operation due to the anonymous nature of the survey. This gives full permission to proceed with the survey as written, with the caveat that any and all changes be reported to HSC by writing within 10 business days. This study is not subject to renewal. The permission letter from HSC is included in the appendix of this document.

3.4 - Data Collection

3.4.1 - Method

Data for this research is collected via online, cross-sectional survey. The 7 questions contained within this survey are mixed among the questions of another researcher to avoid overt knowledge of the purpose to participants. By choosing to distribute this survey via online method, a greater audience population can be reached than more traditional methods. The constant availability of the online survey tailors to the personal time requirements of the participant. An estimation of required time to complete the survey is provided to allow participants the decision of whether or not they want to take the survey.

3.4.2 - Instruments

The online resource of SurveyMonkey is the instrument used for distribution. Participants are instructed to follow a link to the survey and proceed to answer the questions contained within. By using SurveyMonkey, visualization of data is automatically done as survey responses are recorded. This tool also provides direct exportation into Microsoft Excel for further data processing.

3.4.3 - Reliability and Validity

Initial validation of the survey was done by a group of 10 participating students in the College of Business at Idaho State University. Their goal was to take the survey and analyze the flow of questions, looking for typical errors such as spelling, word choice and clarity of questions. They were also asked to provide feedback as to what they thought the survey was measuring. This step was taken to ensure that the questions on the survey were able to gather the information that is needed to identify trends in risk model usage. Since the survey was combined with questions of another researcher at Idaho State University, efforts were taken to ensure that both sets of survey questions were synchronous and not off-putting to the participants. After the students had finished the first round of survey taking, the feedback they provided enabled the survey to be fine-tuned to reflect changes.

The survey was then sent to a representative of ISC^2 for additional validation. She distributed the survey to a small group of approximately 20 professionals, with instructions to take the survey and provide feedback. Results were similar to the student responses from the first round of validation. A major change was made to one of the risk questions to fix an error with the available response choices. This question is shown below:

- **When determining the likelihood of threats to information systems, do you typically base your analysis on a best-guess from previous career experience?**

The question had been mistakenly input as a ranked scale, with choices ranging from "strongly disagree" to "strongly agree." Since this was an incorrect response for this question, it was deleted and re-added to represent the answer choices of "yes", "no", or "no risk management experience."

Before deciding which distribution method to use, research was done into the validity of survey tools available. Research from Marra & Bogue (2006) was used to come to the final decision of using SurveyMonkey, which was picked for the following reasons:

- The tool allows customized layout and welcome pages.
- Automatically differentiates between text and number inputs, and allows questions to only accept certain types of input. This was useful for the first two questions of the survey, which required numerical input.

- Unlimited surveys are allowed within one account, allowing for future distribution to groups outside of ISC^2.
- Data visualization is available from the website interface, eliminating the need to process via Microsoft Excel or other data visualization packages.
- Supports exporting of data into Microsoft Excel and SPSS formats in the event that additional analysis needs to be done on the data.
- Provides the option to distribute anonymous surveys, which was necessary for compliance with Idaho State University's Human Subjects Committee approval of this survey.
- Participant confidentiality is ensured by SurveyMonkey through use of HTTPS encryption on the website and throughout the survey.

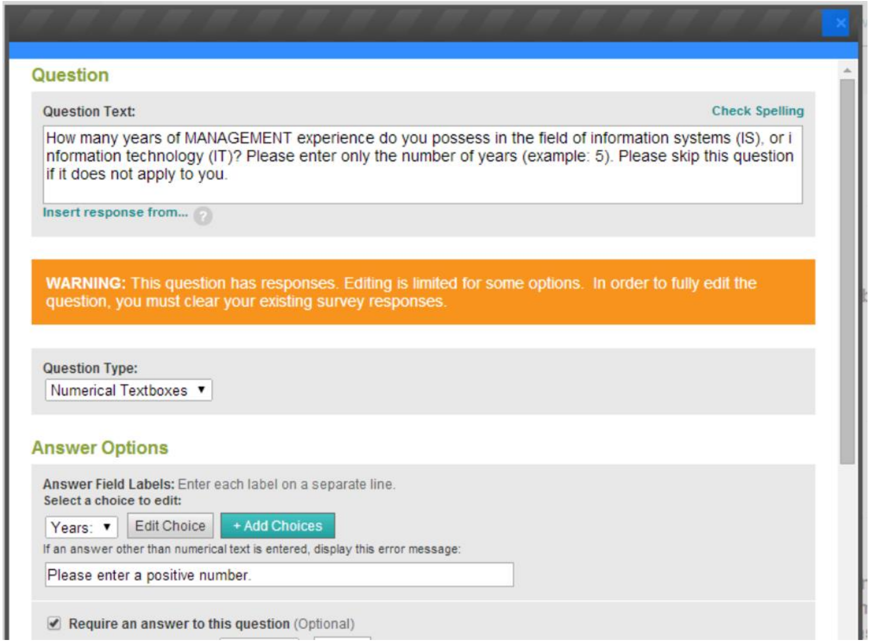
Due to tight time constraints, the reliability of survey responses was not tested in more than the initial two groups. These groups, however, did show consistent answering of the question sets. Despite this initial positive response, the survey still has limitations in the traditional definition of reliability, defined by Wiersma (2011): "a study giving stable results across trials." The reliability of the survey cannot be absolute with only two groups having tested the survey.

3.4.4 – Procedure

A SurveyMonkey account was made for the purposes of this research. This account belongs to the National Information Assurance Training and Education Center (NIATEC) and was created strictly for research purposes. All information related to the survey is documented once this account is accessed through SurveyMonkey's web interface.

The period in which the survey is be considered active for the purposes of this research is from 3/31/14 to 5/1/14. This gives approximately 4 weeks from the time of distribution for participants to take the survey. Follow-up research on data after the end-date may be performed if necessary. Since SurveyMonkey provides 24/7 access to data, the information may be collected for preliminary analysis at any time between the start and end of the survey. The job of converting raw data into useful information is taken care of by the web interface of SurveyMonkey. This avoids the need to export data into processing software, such as Microsoft Excel, unless further analysis is needed.

The process of ensuring that correct responses to the questions are recorded is done through the web interface of SurveyMonkey. The following example shows data input validation on a question within the survey:



Question

Question Text: How many years of MANAGEMENT experience do you possess in the field of information systems (IS), or information technology (IT)? Please enter only the number of years (example: 5). Please skip this question if it does not apply to you.

WARNING: This question has responses. Editing is limited for some options. In order to fully edit the question, you must clear your existing survey responses.

Question Type: Numerical Textboxes

Answer Options

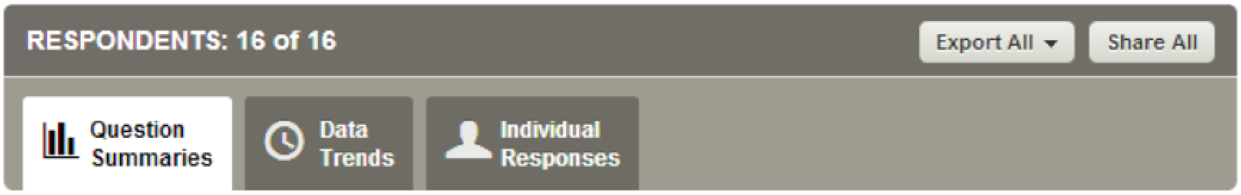
Answer Field Labels: Enter each label on a separate line.

Select a choice to edit: Years:

If an answer other than numerical text is entered, display this error message: Please enter a positive number.

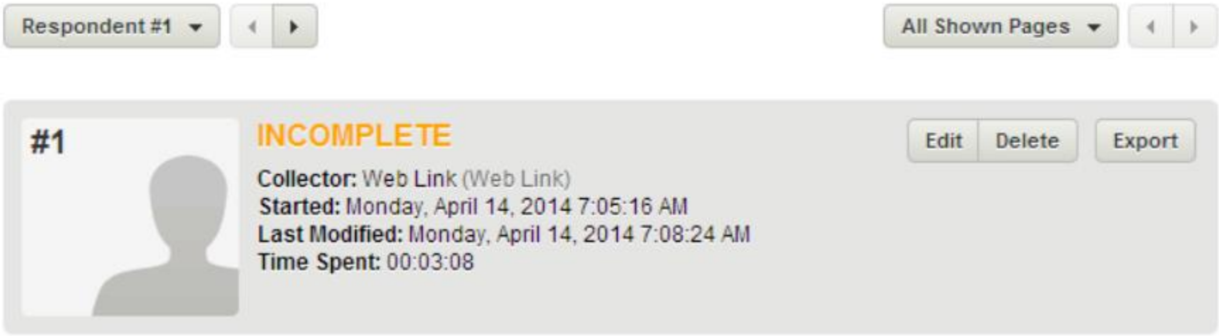
☑ Require an answer to this question (Optional)

Within the SurveyMonkey web interface, results can be viewed using the Analyze Results tab, which provides the following options for data visualization:



Question Summaries provides the actual answers to questions that have been recorded. This enables a global view of how the survey responses develop. It also provides real-time analysis of results, which is helpful in visualization. The Data Trends tab provides a look into the amount of responses that the survey gathers on a defined time-scale. Data frequency has been set to 24 hours, which records all responses within that time period as a count function.

Once gathered, survey data is checked for completeness. The web interface provides a user friendly way to do this, by reporting the status of each survey taken by individual response. These responses are grouped by time taken, but still remain anonymous. The following is an example of output for incomplete surveys:



INCOMPLETE

Collector: Web Link (Web Link)
Started: Monday, April 14, 2014 7:05:16 AM
Last Modified: Monday, April 14, 2014 7:08:24 AM
Time Spent: 00:03:08

Should a participant choose not to complete the survey, then the data is not useful to the research of this study. SurveyMonkey provides a way to delete incomplete responses, by clicking the above button labeled “delete.” Using this method allows us to gather only completed survey responses, thus solving the problem of missing or incomplete data. When data processing is done, all incomplete survey responses are removed via this method.

3.5 - Proposed Statistical Analysis

Once data has been collected from SurveyMonkey, two questions will be analyzed by descriptive statistics and correlation. These questions appear as the first two in the survey, which is found in the appendix. Additionally, correlation analysis will be attempted on the exported responses to these questions, using the statistical software MiniTab. Within the descriptive statistics, only measures of central tendency (mean, median, and mode) will be analyzed. Analysis of standard deviation is not helpful to this analysis because both large and small companies are represented. Because the data collected in response to these questions has the possibility of falling within a very large range, this analysis would not be statistically reliable.

The remaining 5 questions are analyzed specifically for data visualization. By doing this, identification of the primary methods that survey respondents use in performing risk analysis, and whether or not they possess any experience with risk management is accomplished. Should participants answer no to this risk management question, then the results that they provide for the remainder of questions in this survey will be discarded due to lack of usefulness for this research. This is because the study aims at analyzing the methods that IA career professionals use when dealing with risk management. Those who have no experience with this topic will not provide relevant data visualization.

Chapter 4 – Results

4.1 – Introduction

While the ALE formula may provide a simple method of quantifying information systems risk, it may also be the primary method used by certified professionals within ISRM. If subjective opinions are substituted for rigorous mathematical analysis of impact and likelihood, the risk analyst is inadequately valuing expected losses within information systems. Using a singular and subjective approach to risk analysis limits the risk analyst's ability to make accurate predictions and gives management a false sense of security.

The purpose of this chapter is to provide the results that have been obtained from an online, cross-sectional survey about risk analysis methods. Because the survey has not yet ended at the time of this writing, the results presented are a proof of concept to test the hypothesis that the ALE formula is the primary method of quantitative risk analysis used among ISC^2 professionals. Final results will provide a more accurate and robust data set from which to draw conclusions. The results of both visualization and statistical analysis are shown from the preliminary data gathered. These visualizations and results appear in the text of this chapter.

4.2 - Description of Sample

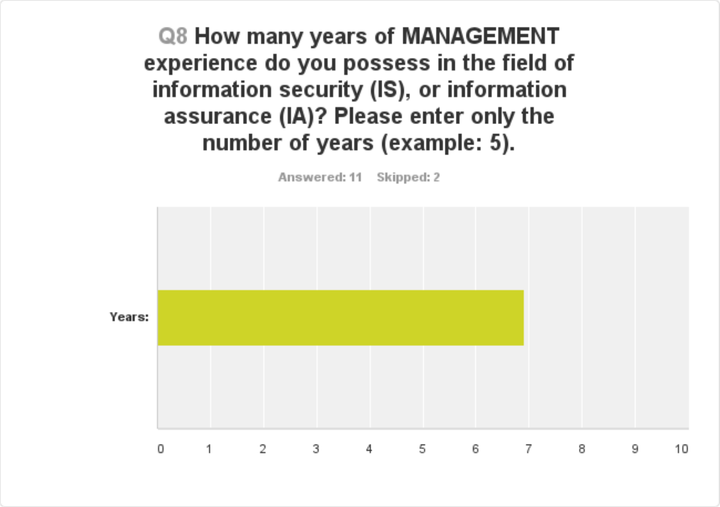
Results from the preliminary data set are representative of the first two days of survey distribution. We expect to see an uptake in survey results as awareness of the survey increases. The target population is over 120,000 ISC^2 members, with no restrictions to country or global location. Thus far, we have obtained 16 responses to the survey. After data cleansing for individuals that did not complete the survey, 13 valid responses remain. This sample represents the following demographics:

- Members of ISC^2.
- Age range of 25 to 54
- 84.62% Male / 15.38% Female
- 61.54% White/Caucasian
- 23.08% Asian or Pacific Islander
- 23.08% Black or African American
- 84.62% from United States
- 7.69% from Europe
- 7.69% from South America
- 76.92% possess Bachelor's Degree, Master's Degree or a combination of the two

4.3 - Statistical Analysis

- **Question 1 – How many years of MANAGEMENT experience do you possess in the field of information security (IS), or information assurance (IA)?**

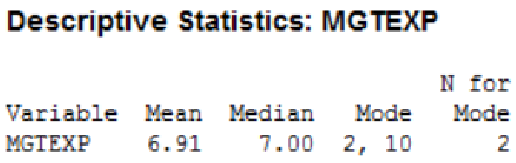
Visualizing the first question through SurveyMonkey's web interface:



Q8 How many years of MANAGEMENT experience do you possess in the field of information security (IS), or information assurance (IA)? Please enter only the number of years (example: 5).

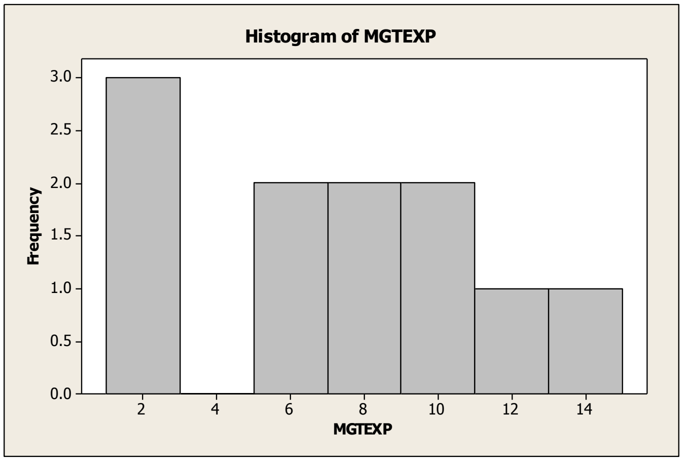
Answered: 11 Skipped: 2

Minitab output of descriptive statistics:



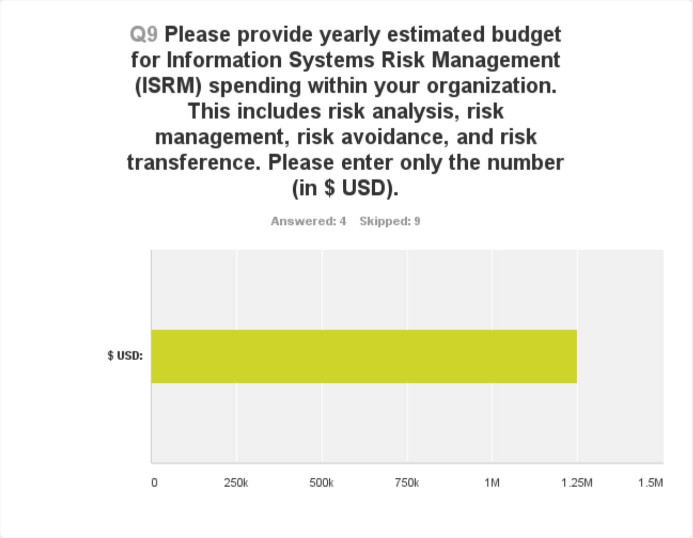
```
Descriptive Statistics: MGTEXP

                                      N for
Variable   Mean   Median    Mode      Mode
MGTEXP     6.91     7.00   2, 10         2
```

Histogram showing frequency of occurrence:



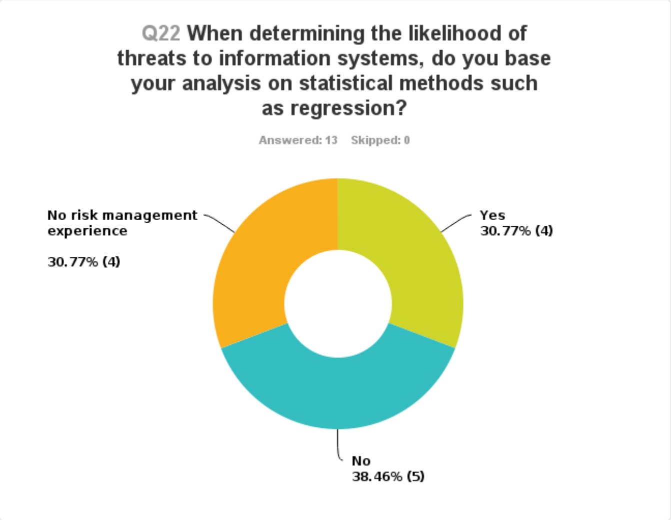
- **Question 2 – Please provide a yearly estimated budget for ISRM spending within your organization. This includes risk analysis, risk management, risk avoidance, and risk transference. Please enter this number in $USD.**

This question was only answered by 4 participants, thus the results are not valid for analysis yet. The following is the visual output from SurveyMonkey:



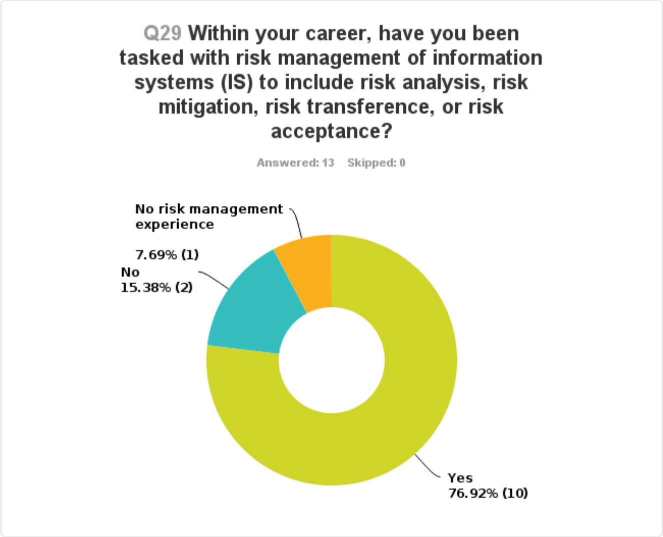
- **Question 3 - When determining the likelihood of threats to information systems, do you base your analysis on statistical methods such as regression?**

Visualization of data from SurveyMonkey's web interface:



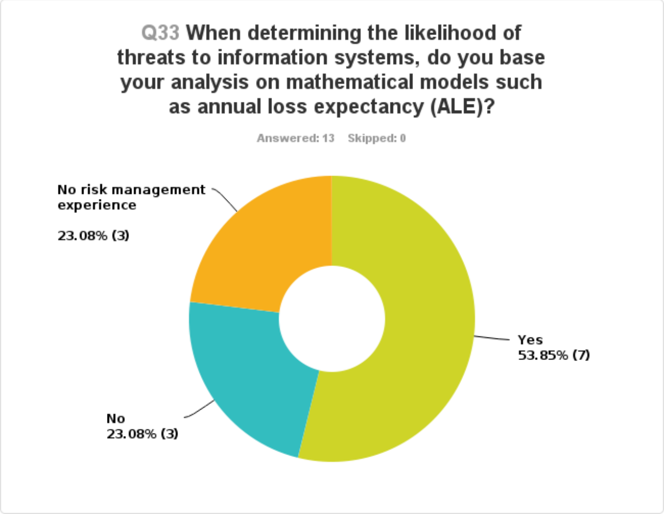
- **Question 4 - Within your career, have you been tasked with risk management of information systems (IS) to include risk analysis, risk mitigation, risk transference, or risk acceptance?**

Data visualization from SurveyMonkey's web interface:



- **Question 5 - When determining the likelihood of threats to information systems, do you base your analysis on mathematical models such as annual loss expectancy (ALE)?**

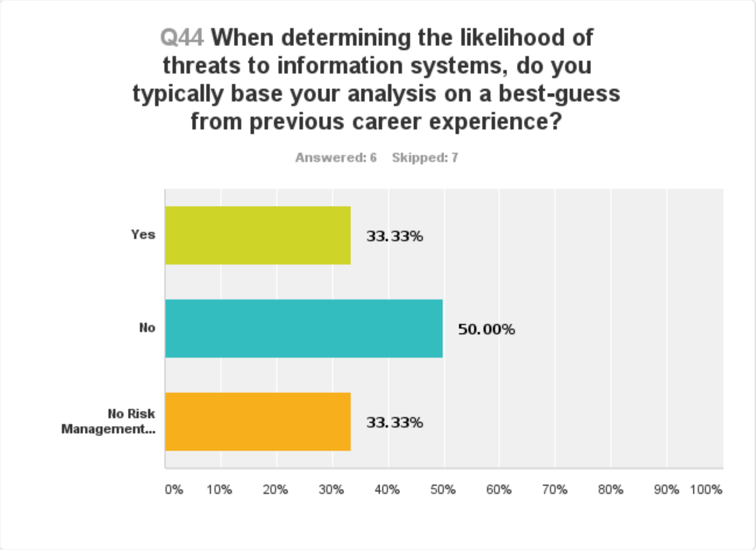
Data visualization from SurveyMonkey's web interface:



Survey results from this question support the hypothesis that ALE is the primary method of use among ISRM professionals surveyed. However, this data is preliminary due to time constraints. As the study concludes, this data will provide a more robust answer.

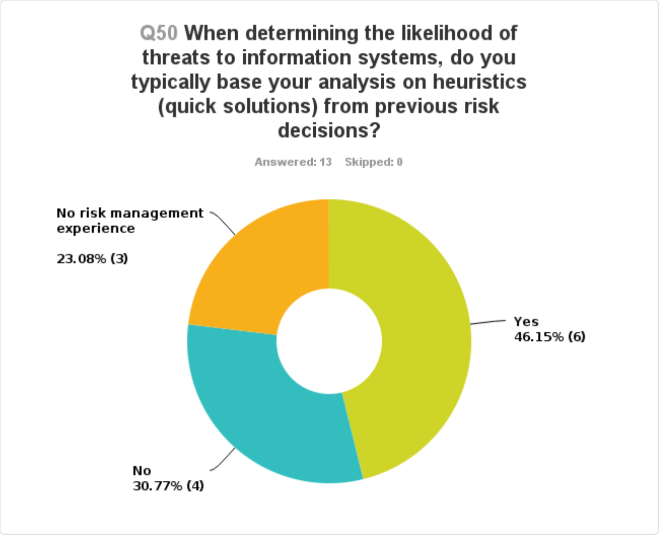
- **Question 6 - When determining the likelihood of threats to information systems, do you typically base your analysis on a best-guess from previous career experience?**

Data visualization from SurveyMonkey's web interface:



- **Question 7 – When determining the likelihood of threats to information systems, do you typically base your analysis on heuristics (quick solutions) from previous risk decisions?**

Data visualization from SurveyMonkey's web interface:



Q50 When determining the likelihood of threats to information systems, do you typically base your analysis on heuristics (quick solutions) from previous risk decisions?

Chapter 5 – Discussion

5.1 - Summary of Major Findings

The purpose of this research is to examine and visualize the realistic usage patterns of the ALE model as compared to other alternatives within ISRM. This is accomplished by analyzing results from an online survey given to ISC^2 members. By doing this, the assumption that ISRM professionals are using the ALE formula as a primary method of quantitative risk analysis is tested. Literature review provides alternatives to the singular approach of ALE. These alternatives combine the reduction of subjectivity with unique approaches to risk analysis that cross reference other career fields, such as biology, finance, and computer science. Relevant frameworks are introduced to show that currently accepted risk management strategies allow the ALE formula as a method of quantitative analysis.

The methodology for this study was designed to support a cross-sectional, online survey distributed through SurveyMonkey's website. The results of both survey and literature review aim to answer the following research questions:

1. Among the surveyed population, is usage of the ALE quantitative risk analysis formula greater than that of statistical methods, best-guess analysis, or heuristics?
2. Do years of management experience within the IA or IS field correlate with the yearly estimate of annual spending on ISRM?
3. Are there alternative methods to ALE for quantifying information systems risk?

Preliminary results from the online survey have been analyzed, providing a proof of concept visualization strategy. These visualizations, as presented in the Analysis chapter, support the hypothesis that ALE is the primary method of quantitative risk analysis used among the survey participants (54%). This is limited by the small amount of data, so this hypothesis test is not as robust as it will be when the survey ends. The survey also shows that the next most popular method of risk analysis is that of heuristics, or quick decisions from previous risk analyses within career experience (46%).

5.1.1 – Discussion

Based on the preliminary findings of the survey, ALE is the primary method of quantitative risk analysis used by the surveyed population of ISRM professionals. Because they are taught the ALE method when preparing for certification within ISC^2, they primarily use ALE as an approach to quantitative risk management. This assertion comes with the limitations of preliminary data. As survey responses are collected, these findings may change.

The literature review shows that ALE is a useful method of quantitative risk analysis only when rough estimation is necessary. The strength of ALE can be improved by a reduction in subjective opinions about the likelihood of impact and consequence. Rigorous mathematical analysis, such as probability determination, adds objectivity to the ALE formula. However, given the vast amount of alternatives to quantitative risk analysis, ALE should be used in combination with other methods outlined in the Literature Review. By doing this, organizations develop a portfolio of risk management approaches to provide defense-in-depth and defense-in-breadth to the organization. Regardless of which approaches are chosen, the organization must define and take on certain levels of acceptable risk with each alternative.

The practical implications of this research may expose a growing problem with professionals in the IA career field. Since they are taught limited approaches to quantitative risk analysis, they may implement these before doing deeper research into alternatives. This may reduce the effectiveness of ISRM as an industry, due to the large number of certified professionals in the workforce.

5.2 - Future Research

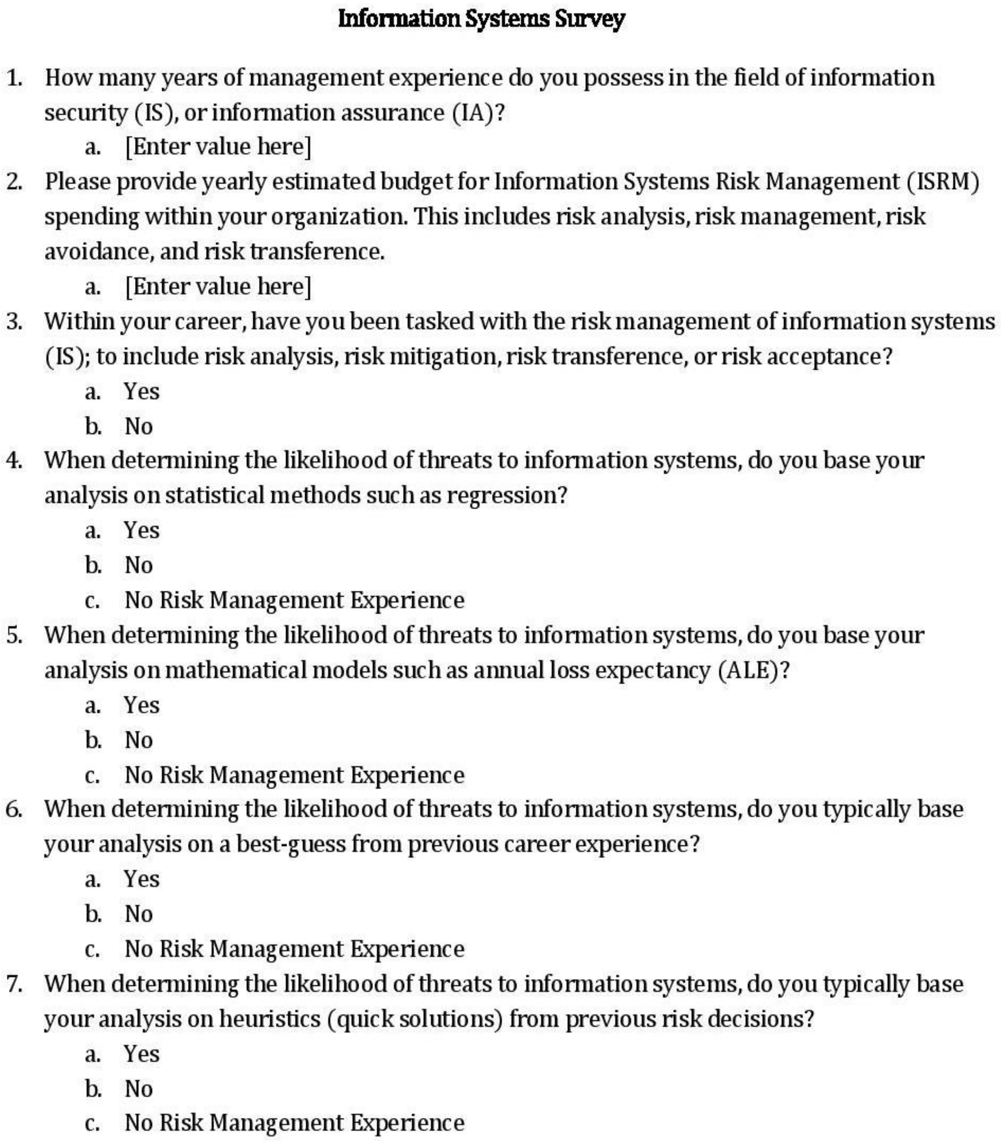
As this research has progressed, topics for future research have surfaced as the following:

- Development of ISRM portfolios that mimic the efficient frontier of Markowitz's theory of Portfolio Selection. By doing this, organizations can develop tailored approaches for risk management based on their own values, beliefs, and goals.
- The use of linear regression to estimate ISRM spending based on predefined variables. This would develop another alternative to the ALE formula.
- Development of a software package that offers choices of different methods of quantitative risk analysis. This would take the mathematical rigor out of quantitative risk analysis, and make it more accessible to ISRM professionals.
- Developing a framework to measure how often subjective opinions are used determining the likelihood and impact within the ALE risk quantification

model. This would expand upon the research in this paper and test the hypothesis of over-reliance within ISRM professionals.

Appendix

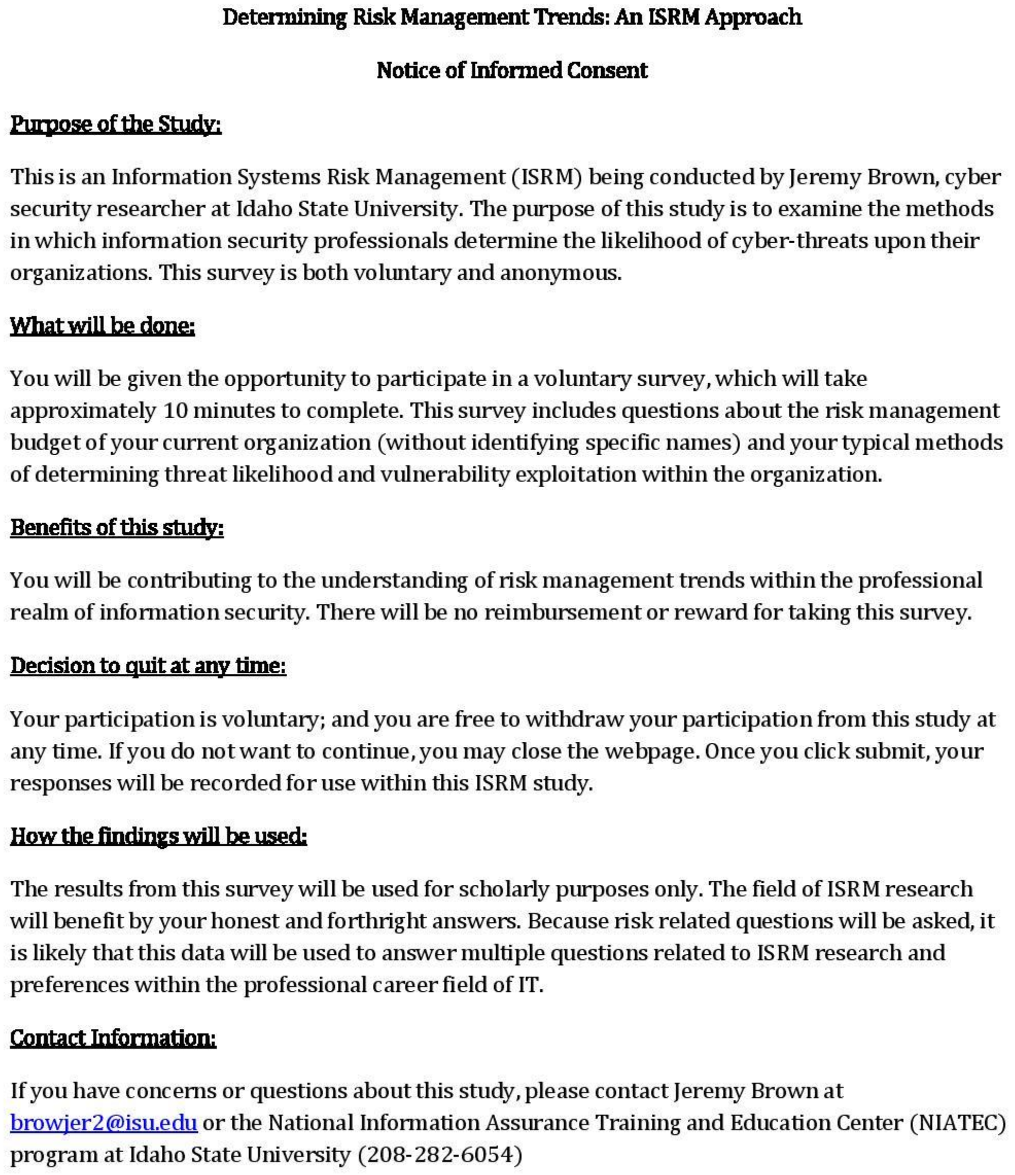
Figure 1 – Questions given to survey participants.



Information Systems Survey

1. How many years of management experience do you possess in the field of information security (IS), or information assurance (IA)?
   a. [Enter value here]
2. Please provide yearly estimated budget for Information Systems Risk Management (ISRM) spending within your organization. This includes risk analysis, risk management, risk avoidance, and risk transference.
   a. [Enter value here]
3. Within your career, have you been tasked with the risk management of information systems (IS); to include risk analysis, risk mitigation, risk transference, or risk acceptance?
   a. Yes
   b. No
4. When determining the likelihood of threats to information systems, do you base your analysis on statistical methods such as regression?
   a. Yes
   b. No
   c. No Risk Management Experience
5. When determining the likelihood of threats to information systems, do you base your analysis on mathematical models such as annual loss expectancy (ALE)?
   a. Yes
   b. No
   c. No Risk Management Experience
6. When determining the likelihood of threats to information systems, do you typically base your analysis on a best-guess from previous career experience?
   a. Yes
   b. No
   c. No Risk Management Experience
7. When determining the likelihood of threats to information systems, do you typically base your analysis on heuristics (quick solutions) from previous risk decisions?
   a. Yes
   b. No
   c. No Risk Management Experience

Figure 2 – Informed Consent given to participants of the study.



Determining Risk Management Trends: An ISRM Approach

Notice of Informed Consent

Purpose of the Study:

This is an Information Systems Risk Management (ISRM) being conducted by Jeremy Brown, cyber security researcher at Idaho State University. The purpose of this study is to examine the methods in which information security professionals determine the likelihood of cyber-threats upon their organizations. This survey is both voluntary and anonymous.

What will be done:

You will be given the opportunity to participate in a voluntary survey, which will take approximately 10 minutes to complete. This survey includes questions about the risk management budget of your current organization (without identifying specific names) and your typical methods of determining threat likelihood and vulnerability exploitation within the organization.

Benefits of this study:

You will be contributing to the understanding of risk management trends within the professional realm of information security. There will be no reimbursement or reward for taking this survey.

Decision to quit at any time:

Your participation is voluntary; and you are free to withdraw your participation from this study at any time. If you do not want to continue, you may close the webpage. Once you click submit, your responses will be recorded for use within this ISRM study.

How the findings will be used:

The results from this survey will be used for scholarly purposes only. The field of ISRM research will benefit by your honest and forthright answers. Because risk related questions will be asked, it is likely that this data will be used to answer multiple questions related to ISRM research and preferences within the professional career field of IT.

Contact Information:

If you have concerns or questions about this study, please contact Jeremy Brown at browjer2@isu.edu or the National Information Assurance Training and Education Center (NIATEC) program at Idaho State University (208-282-6054)

References

401k, Smart. *Modern portfolio theory and the efficient frontier.*

Abramov, Rafail V., and Andrew J. Majda. "Quantifying uncertainty for non-gaussian ensembles in complex systems." *SIAM Journal of Science and Computing*, 2004: 411-447.

Ahn, Mark J., and William D. Falloon. *Strategic Risk Management.* Chicago, Illinois: Probus Publishing Company, 1991.

Ali, Dana, and Goran Kap. *Statistical analysis of computer network security.* Masters Thesis, Stockolm, Sweden: KTH Royal Institute of Technology, 2013.

Asosheh, Abbas, Bijan Dehmoubed, and Amir Khani. *A new quantitiative approach for information security risk assesment.* Risk Model, Richardson, TX: Institute for Scientific Information, 2009.

Baruch, Yehuda, and Brooks C. Holtom. "Survey response rate levels and trends in organizational research." *Human Relations* (SAGE Publications), 2008: 1139-1160.

Bernstein, Peter L. *Against The Gods.* New York: John Wiley & Sons, INC., 1996.

Bodin, L., L. Gordon, and M. Loeb. "Evaluating information security investments using the analytiic heirarchy." *Community of the ACM*, February 2005: 461-485.

Bodin, Lawrence D., Lawrence A. Gordon, and Martin P. Loeb. "Information security and risk management." *Communications of the ACM*, April 1, 2008: 64-68.

Braber, Folker D, Ida Hogganvik, Mass S Lund, Ketil Stolen, and Fredrik Vralsen. "Model-based security analysis in seven steps - a guided tour to the CORAS method." *BT Technology Journal* 25, no. 1 (January 2007): 101-117.

Chen, Gang, and Dawei Zhao. "Model of information security risk assessment based on improved wavelet neural network." *Journal of Networks*, 2013: 2093-2100.

Cleghorn, Lance. "Network defense methodology: a comparison of defense in depth and defense in breadth." *Journal of Information Security*, 2013: 144-149.

Covello, Vincent T, and Jeryl Mumpower. *Risk analysis and risk management: an historical perspective.* Chicago: Society for Risk Analysis, 1985.

Fermat, Pierre de. *Untitled letter to pascal on the subject of probability.* Letter, Pierre de Fermat, 1654.

Fischhoff, Baruch, Sarah Lichtenstein, Paul Slovic, Stephen L. Derby, and Ralph L. Keeney. *Acceptable Risk.* Cambridge: Cambridge University Press, 1981.

Gran, Bjorn Axel. *CORAS: a platform for risk analysis of security critical systems.* Regenburg, GER, January 22, 2002.

Gregg, Michael. *CISSP exam cram 2.* Indianapolis, IN: Que Publishing, 2005.

Hogganvik, Ida, and Ketil Stolen. "A graphical approach to risk identification, motivated by emperical investigations." *MoDELS, LNCS 4199*, 2006: 574-588.

Information Technology Laboratory. *Guide For Applying the Risk Management Framework to Federal Information Systems.* Gathersburg: National Institute of Standards and Technology, 2010.

International Information Systems Security Certification Consortium. *ISC2 members in "good standing".* January 1, 2014. https://www.isc2.org/MembersInGoodStanding.aspx (accessed March 2, 2014).

International Standards Organization. *ISO/Guide 73:2009(en).* November 13, 2009. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en (accessed April 7, 2014).

International Standards Organization. *ISO/IEC 27005 : Information Security Risk Management.* June 30, 2008.

Investopedia. *Return on Investment - ROI.* January 1, 2014. http://www.investopedia.com/terms/r/returnoninvestment.asp (accessed March 28, 2014).

Landoll, Douglas J. *The Security Risk Assessment Handbook.* Boca Raton, FL: Taylor & Francis Group, 2006.

Lei, Pan. "Dynamic Evaluation Model of Security Risk in Information Systems." *International Conference on Computer Science and Electronics Engineering.* Guang Han: IEEE, 2012. 225 - 229.

Maconachy, Victor W., Corey D. Schou, and Daniel Ragsdale. "A model for information assurance: an integrated approach." *IEEE Workshop on Information Assurance and Security.* West Point, NY: IEEE, 2001. 306-310.

Markowitz, Harry M. *Portfolio selection: efficient diversification of investments.* New York: John Wiley & Sons, 1959.

Markowitz, Harry. "Portfolio Selection." *The Journal of Finance*, 1952: 77-91.

Marra, Rose M, and Barbara Bogue. "A critical assessment of online survey tools." *WEPAN Conference.* Columbia, MO: University of Missouri, 2006. 1-11.

McFarlan, Warren F. "Portfolio approach to information systems." In *Catching up with the computer revolution*, by Harvard Business Review, 179-193. Boston, MA: John Wiley & Sons, 1983.

Mercuri, Rebecca T. "Analyzing Security Costs." *Security Watch*, June 1, 2003: 15-18.

National Institute of Standards and Technology. *FIPS pub 199: Standards for security categorizations of federal information and information systems.* Government Standard, Gaithersburg, MD: United States Department of Commerce, 2004.

National Institute of Standards and Technology. *Guideline for the analysis of local area network security.* Government Standard, Washington, DC: United States Department of Commerce, 1994.

National Institute of Standards and Technology. *NIST special publication 800-30 revision 1 - guide for conducting risk assessments.* Washington DC: United States Department of Commerce, 2012.

Quinlan, J.R. *Induction of Decision Trees.* Boston: Kluwer Academic Publishers, 1986.

Rajbhandari, Lisa, and Einar Snekkenes. "Intended Actions: Risk Is Conflicting Incentives." Norwegian Information Security Laboratory - Gjovik University College, September 5th, 2012.

Ryan, Julie J.C.H., and Daniel J. Ryan. "Expected benefits of information security benefits." *Elsevier - Science Direct*, August 3, 2006: 579-588.

Saaty, R.W. "The analytic hierarchy process—what it is and how it is used." *Mathematical Modelling*, 1987: 161-176.

Tamijidyamcholo, Alireza, and Rawaa Dawoud Al-Dabbagh. "Genetic Algorithm Approach for Risk Reduction of Information Security." *International Journal of Cyber-Security and Digital Forensics*, 2012: 59-66.

United States Department of Commerce. *FIPS guideline for automatic data processing risk analysis.* Printed Report, Springfield, VA: National Bureau of Standards, 1979.

Wiersma, Wybo. "The validity of surveys: online and offline." Research Article, 2011.

Zhang, Jun, Gilbert G. Walter, Yubo Miao, Wan Ngai, and Wayne Lee. "Wavelet neural networks for function learning." *IEEE Transactions on Signal Processing*, 1995: 1485-1497.