

SECURITY RISK ANALYSIS AND CRITICAL INFORMATION SYSTEMS

A THESIS SUBMITTED TO THE COLLEGE OF BUSINESS ADMINISTRATION AT
HAWAI'I PACIFIC UNIVERSITY IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN

INFORMATION SYSTEMS

FALL 2011

BY

PHILIP W. ROBBINS

Abstract

Security Risk Analysis and Critical Information Systems

Philip Robbins, BSEE, PMP, CISSP

M.S. Information Systems, Hawaii Pacific University,
Department of Information Systems

December 2011

Thesis Advisor: Dr. Kenneth Rossi, Ed.D.

This content analysis study examines the Information Systems Security Engineering domain, existing Risk Management Framework (RMF) processes, and specific Security Risk Analysis (SRA) approaches as it pertains to the Information Assurance (IA), and security of Critical Information Systems (CIS), supporting missions of ranging criticality categories processing, transmitting, and handling information of various classification levels. Risk determinations made by approving authorities benefit from a truly quantitative and blanket risk decision metric for CIS. A proposed metric is formulated by defining a continuous, time-dependent risk function based on multivariate analysis, probability distribution theory, and basic sensitivity analysis. This determination metric further serves as the basis for a proposed RMF that is based on existing Federal guidelines, Department of Defense instructions, policies, and guidance; supported through the analysis of modeled samples, incorporating modified IA constraints, similarly found with CIS operating at Combatant Commands/Services/Agencies.

Security Risk Analysis and Critical Information Systems

Certification Page

Security Risk Analysis and Critical Information Systems

The thesis submitted by Philip W. Robbins has been reviewed and approved by the Hawai'i Pacific University College of Business Administration, Department of Financial Economics and Information Systems.

Kenneth G. Rossi, Ed.D., Thesis Advisor
Assistant Professor, Information Systems

Date

Lawrence Rowland, Ed.D., Reader
Assistant Professor, Information Systems

Date

Richard Chepkevich, Reader
Instructor, Information Systems

Date

Dedication

To those in my life.

Acknowledgements

I would like to thank the following at Hawaii Pacific University (HPU) whose direction, guidance, and teachings greatly contributed to the writing of this paper:

Dr. Cathrine Linnes, Ph.D.	Associate Professor, HPU
Dr. Kenneth Rossi, Ed.D.	Assistant Professor, HPU
Dr. Lawrence Rowland, Ed.D.	Assistant Professor, HPU
Mr. Richard Chepkevich	Instructor, HPU

Special acknowledgement is given to the following who continue to be a personal source of inspiration and motivation. Their encouragement and support of my academic endeavors, as well as, my career within the field of Information Systems Security, continues to be a powerful catalyst for excellence.

Mr. Randall Cieslak, SES	Chief Information Officer, USPACOM Information Systems Authorizing Official
Mr. Terry Scott, GS-15	Deputy Director for Communications, USPACOM
Col Douglas Mason, USMC	Division Chief for Communications, USPACOM
LTC Wayne Siebert, USA	<i>Former</i> Cyber Security Branch Chief, USPACOM
Ms. Leona Bangerter, GS-14	Comm Sys Integration Branch Chief, USPACOM
Ms. Juliet Eiselstein, GS-14	Cyber Security Deputy Branch Chief, USPACOM Information Assurance Manager
Mr. Joshua Margolin, GS-13	C&A Section Chief, USPACOM
Mr. Rob Mathieson, GS-13	CND Section Chief, USPACOM
Mr. Jake Ross, GS-13	Computer Network Defense Analyst, USPACOM
Mr. Scott Atta, GS-13	Computer Network Defense Analyst, USPACOM

Table of Contents

List of Tables.....	iii
List of Figures.....	iv
List of Symbols.....	v
List of Abbreviations.....	vi
 Chapter 1 – INTRODUCTION	
Background.....	1
Purpose of the Study.....	3
Problem Statement.....	4
Research Questions.....	5
Method of Inquiry.....	6
Assumptions.....	8
Limitations.....	8
Delimitations.....	9
Paper Organization.....	10
 Chapter 2 – LITERATURE REVIEW	
Purpose of the Chapter.....	11
Organization of the Chapter.....	12
History of Security Risk Analysis.....	12
Problem Breakdown.....	13
Review.....	20
Summary.....	21
 Chapter 3 – METHODOLOGY	
Purpose of the Chapter.....	22
Organization of the Chapter.....	22
Technique.....	23
Data.....	41
Procedure.....	50
Assumptions.....	52
Research Questions / Test Methods.....	53
Strengths.....	54
Weaknesses.....	54
Chapter Summary.....	55
 Chapter 4 – ANALYSIS	
Purpose of the Chapter.....	56
Chapter Organization.....	57
Preliminary Analysis.....	58

Descriptive Statistics.....	58
Reliability.....	71
Research Questions / RQ1 Results.....	73
Research Questions / RQ2 Results.....	85
Chapter Summary.....	90
Chapter 5 – CONCLUSION	
Purpose of the Chapter.....	92
Chapter Organization.....	92
Findings.....	93
Conclusions.....	95
Recommendations for use of Results.....	96
Recommendations for Future Research.....	97
Summery.....	98
Appendix	
List of Equations.....	99
References.....	106

List of Tables

Table 1.	DoDI 8510.01 Severity Categories and Associated Impact Factors.....	34
Table 2.	MAC and Associated Risk Dimensions for Risk Determination Metric.....	38
Table 3.	DoDI 8500.2 Controls for Classified Systems.....	42
Table 4.	Possible IA Constraints for CIS.....	45
Table 5.	CIS Test Models and Qualitative DIACAP IA Scorecard Data Sample.....	48
Table 6.	Coefficient Values for the Conditional Probability of an Attack.....	75
Table 7.	Component Behavior of a Quantitative Risk Expression Truth Table.....	77

List of Figures

Figure 1.	SRA-CIS Work Breakdown Structure.....	8
Figure 2.	Probability Bounds.....	17
Figure 3.	CIA Information Security Triad.....	31
Figure 4.	Risk Logic Diagram for CIS.....	35
Figure 5.	US-CERT Vulnerability Plot.....	39
Figure 6.	US-CERT Threat Incident Plot.....	40
Figure 7.	Expected Value and Risk Loss Confidence vs Cumulative Risk Product....	60
Figure 8.	IAS (s = 1, 2, 3) Probability-Impact Tree Diagram for Confidentiality.....	63
Figure 9.	IAS (s = 4, 5, 6, 7) Probability-Impact Tree Diagram for Confidentiality...	64
Figure 10.	IAS (s = 1, 2, 3) Probability-Impact Tree Diagram for Integrity.....	65
Figure 11.	IAS (s = 4) Probability-Impact Tree Diagram for Integrity.....	66
Figure 12.	IAS (s = 5, 6, 7) Probability-Impact Tree Diagram for Integrity.....	67
Figure 13.	IAS (s = 1, 2) Probability-Impact Tree Diagram for Availability.....	68
Figure 14.	IAS (s = 3) Probability-Impact Tree Diagram for Availability.....	69
Figure 15.	IAS (s = 4, 5, 6, 7) Probability-Impact Tree Diagram for Availability.....	70
Figure 16.	CIS Test Model Analysis: 01/Y.....	78
Figure 17.	CIS Test Model Analysis: 02/CQRSTUVWIJKP.....	78
Figure 18.	CIS Test Model Analysis: 22/CQRSTUIJK.....	78
Figure 19.	CIS Test Model Analysis: 40/BQRSTUVWIJK.....	79
Figure 20.	CIS Test Model Analysis: 62/AQRSTUVWIJK.....	79
Figure 21.	CIS Test Model Analysis: 74/BCQRSTUJ.....	79
Figure 22.	CIS Test Model Analysis: 90/ABQRSTUVWJ.....	80
Figure 23.	CIS Test Model Analysis: 91/BCQRSTUVWIJKP.....	80
Figure 24.	CIS Test Model Analysis: 92/BCQRSTUVWIJKXP.....	80
Figure 25.	CIS Test Model Analysis: 93/CQRSTUVWIJK.....	81
Figure 26.	CIS Test Model Analysis: 96/CQRSTUVWK.....	81
Figure 27.	CIS Test Model Analysis: 97/BQRSTUVWIJKX.....	81
Figure 28.	CIS Test Model Analysis: 98/BQRSTUVWIX.....	82
Figure 29.	CIS Test Model Analysis: 99/BQRSTUVWJX.....	82
Figure 30.	CIS Test Model Analysis: 100/BQRSTUVWKX.....	82
Figure 31.	CIS Test Model Analysis: 101/AQRSTUVWIJKX.....	83
Figure 32.	CIS Test Model Analysis: 102/AQRSTUVWI.....	83
Figure 33.	CIS Test Model Analysis: 103/AQRSTUVWJX.....	83
Figure 34.	CIS Test Model Analysis: 104/AQRSTUVWKX.....	84
Figure 35.	CIS Test Model Analysis: 106/Z.....	84
Figure 36.	Risk Determination Curve: Maximum Boundary Over Time.....	87
Figure 37.	Risk Determination Tolerances.....	89
Figure 38.	Risk Areas as a function of Probability and Impact.....	90

List of Symbols

A	CIA security triad (risk dimension) upper summation constant
B	information assurance services upper summation constant
C	risk element index upper summation function
C_{TOTAL}	total population / distinguishable combinations
D_i	indexed event description
E_i	indexed event
δ	control variable
δ_i	control element
e	level of precision / confidence interval for sample
f	function of
γ	confidence factor
L	likelihood function
i	risk element index
λ	vulnerability variable
λ_i	vulnerability element
n	risk dimension index
n	information security service
Ω	risk element set
Ω_i	indexed risk element
Ω_c	risk component
Ω_{sc}	limited set of risk components
P	probability
P^*	bayes' likelihood formula
P_i	risk element probability
p	sample degree of variability
R	risk variable
R_{LC}	risk loss confidence
R_{EV}	expected value of risk
σ	standard deviation between CIS model samples and total constraints
s	information assurance service (IAS) index
s	test model sample size
θ	threat variable
θ_i	threat element
U	universal set
ω	impact variable
ω_{CAT}	impact severity category
ω_i	impact element
Z	probability / confidence of the sample distribution (Z-value)

List of Abbreviations

ARO	Annual Risk Occurrence
ATO	Authority to Operate
ALE	Annualized Loss Expectancy
C	Compliant
C&A	Certification & Accreditation
C2	Command & Control
CAT	Category
CC/S/A	Combatant Commanders/Services/Agencies
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CIS	Critical Information Systems
CISSP	Certified Information Systems Security Professional
CND	Computer Network Defense
CNSSI	Committee on National Security Systems Instruction
DAA	Designated Approving Authority
DIACAP	Department of Defense Information Assurance Certification & Accreditation Process
DoD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DV	Dependent Variables
EF	Exposure Factor
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTA	Fault Tree Analysis
GS	General Schedule
HPU	Hawaii Pacific University
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAS	Information Assurance Services
IE	Initiating Event
ISS	Information Security Services
ISD	Information Service Domain
INFOSEC	Information Systems Security
IT	Information Technology
ITTO	Inputs, Tools, Techniques, and Outputs
IRM	Information Risk Management
IS	Information Systems
ISO	International Organization for Standardization
ISSE	Information Systems Security Engineering
ISSEP	Information Systems Security Engineering Professional
ITTO	Inputs, Tools & Techniques, and Outputs

IV	Independent Variables
MAC	Mission Assurance Category
MVA	Multivariate Analysis
N/A	Not Applicable
NC	Non-Compliant
NISSC	National Information Systems Security Conference
NIST	National Institute of Standards and Technology
PAA	Principal Accrediting Authority
PCA	Principal Component Analysis
PDF	Probability Distribution Functions
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMP	Project Management Professional
POA&M	Plan of Action and Milestones
PRA	Probabilistic Risk Assessment
RMF	Risk Management Framework
SES	Senior Executive Service
SLE	Single Loss Expectancy
SRA	Security Risk Analysis
SRA-CIS	Security Risk Analysis and Critical Information Systems
US	United States
USG	United States Government
USPACOM	United States Pacific Command
VMS	Vulnerability Management System
WBS	Work Breakdown Structure

CHAPTER 1

INTRODUCTION

Background

Technology is everywhere and information is power. Information Systems (IS) use technologies that allow information to be transmitted, stored, and accessed nearly instantaneously, in what has become an age of modern communications and global interconnectedness. The strategic use of Information Systems, within enterprise business environments, not only provides a competitive edge, but is quickly being regarded as a resource of necessity rather than of convenience, in surviving what is now considered, a globalized marketplace (Schilling, 2009). Critical Information Systems (CIS) are systems operated by the Department of Defense (DoD) that processes information which would have a debilitating impact on the mission of the DoD (Section 3541 Title 44 U.S.C., 2002). The use of CIS, or National Security Systems, by the United States Government (USG) is absolutely essential, from conducting daily tasks, to providing Command and Control (C2) of military forces, national security intelligence and cryptologic activities, and is an integral part of weapons and war fighter operations (NIST SP 800-59, 2003).

Military operations not only depend on well trained troops but advanced technologies that enable the effective communication and sharing of critical information. In the past scouts were deployed to gather and transport vital information. To anticipate an enemy's next move or to quickly get a grasp of a situation can make the difference between success and failure.

The fact that superior situational awareness is the key to success is even truer today than ever before. Today, the role of information has expanded into information dominance and cyber warfare, creating a completely new realm for exerting control over an enemy, the same way land, sea, air, and space are considered major military realms (Endsley, 1997).

Of critical importance is the ability of the USG to adequately protect its information and information systems (PDD 63, May). Security is an important attribute of information systems. Data owners have a responsibility for the Information Assurance (IA), and adequate protection, of their information and critical information systems from unauthorized disclosure, modification, and disruption, in order to ensure confidentiality, integrity, and availability. This involves analyzing protection needs, defining security requirements, and identifying security controls; ensuring that security is included throughout the entire life-cycle of those systems (Hansche, 2005).

In 2002, the Federal Information Security Management Act (FISMA) was put into law recognizing the increased reliance on automated and interconnected information systems to perform functions essential to national security. FISMA holds the head of each Federal agency responsible for establishing an information security program, that provides sufficient protections consistent with the risk and magnitude of impact resulting from the unauthorized access or tampering of systems, processing information operated by the DoD (44 U.S.C. § 3541). Information Risk Management (IRM) is considered a central part of an Information Security / Assurance program that allows organizations to methodically identify, assess, and treat negative risks associated with the operation of Critical Information Systems.

Despite massive investments in security technology, information is never truly secure where it resides. For most organizations, the value of the information associated with an IS

exceeds the value of the security technology associated with the IS, although, the resources and costs in maintaining compliance, while keeping up with the never ending flow of regulatory requirements, can be overwhelming. A discussion based on risk is empowering. It helps align security investments to what is driving the organization. It is important for an organization to take into account what risk might mean to their strategies, and the outcomes those strategies will produce, while calibrating an appropriate balance between risk and reward that corresponds with the organization's appetite for risk and mission success.

Purpose of the Study

In the particular case of Information Systems, there has been a reluctance to tackle the subject of risk due to perceived complexities and inexactness. With its growing importance, Critical Information Systems should be made subject to appropriate risk analysis and risk management techniques (Birch, 1992). Security Risk Analysis (SRA) is a technique used in Information Risk Management as a method of identifying threats, vulnerabilities, and possible impact to determine security controls for critical information systems. The purpose of SRA is to assist managers in making informed decisions. There are varying degrees of SRA, each providing differing views of an organization's risk posture. There are two types of SRA approaches: Qualitative Assessments and Quantitative Analysis (Schreider, 2003). Each approach has its own pros and cons, applying more appropriately to some situations than others. Qualitative Risk Assessments use judgment and intuition instead of numbers - evaluating threat scenarios and rating the probability, potential loss, and severity of each threat based on experience.

If risks are only identified, and not quantified, decisions under uncertainty become

intuitive and speculative. Identified risks are better quantified as the resulting credibility and quality of decisions made are significantly enhanced. It is essential that risks for CIS are adequately managed, and, for this purpose, risks must be quantified. Quantitative risk analysis assigns real and meaningful numbers to all elements of the risk analysis process. These elements may include safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, etc. Quantitative risk analysis also provides concrete probability percentages when determining the likelihood of threats. Only when all of these are quantified, is the process said to be quantitative (Harris, 2008).

The objectives of this paper were to advance the discussion of Security Risk Analysis and Critical Information Systems (SRA-CIS), by (i) proposing a quantitative time-dependent risk expression, (ii) derive a corresponding quantitative risk determination metric for the operation of Critical Information Systems by approving authorities, and finally, (iii) propose the integration of these results into a RMF tailored for Combatant Commanders / Services / Agencies (CC/S/A). The relevance and implications of building on modern risk theory to derive unique measures of risk for CIS is further discussed within the concluding section in Chapter 5.

Problem Statement

Decisions are complicated, and as such, it is important that an organization have the best possible information on risks. If you accept the argument that risk matters, and that it affects how senior management make decisions, it follows logically that measuring risk is a critical step towards managing it (Birch, 1992). To this end, the discussion of the core problem surrounding SRA-CIS, namely, the absence of a truly quantitative risk expression and

blanket risk decision metric for critical information systems is developed.

To make responsible risk management decisions it is important to avoid overreaction, but equally important, as not to systematically disregard the full spectrum of risk elements for lack of empirical evidence. Unfortunately, the dialogue regarding SRA-CIS is riddled with rhetoric; lacking a comprehensive and commonly agreed upon SRA method for CIS. As a result, conventional risk management decisions are made in the absence of formal quantitative risk framework.

Research Questions

The principal aim of this paper is to achieve a greater understanding of SRA-CIS by addressing the following research questions:

- Q1. Is it possible to create a meaningful continuous, time-dependent, quantitative risk expression for CIS given existing security risk analysis (SRA) techniques?
- Q2. Is it possible to create a meaningful continuous, time-dependent, quantitative risk determination metric for CIS from a risk expression?

In being able to answer these research questions, a thorough and complete literature review has been conducted on the of subject risk, as it pertains to the field of CIS. Much is written on the general subject of risk, however, literature that specifically ties risk to CIS is mostly limited to DoD guidance and instructions which, in turn, provides the bulk of answers to many subsequent questions that surface when addressing risk within the field of CIS, namely: (i) what is *risk*?; (ii) what is *confidence* and *uncertainty*, its relationship with each other, and with risk?; (iii) what are the properties (variables and elements) of risk?; (iv) what are *threats*, *vulnerabilities*, *IA controls*, *impact*, its relationship with risk, associated dependencies,

competing constraints with other risk elements, and behavioral model with respect to time?; (v) what are the risks associated with the operation of critical information systems?; (vi) how does information *confidentiality*, *integrity*, and *availability* influence risk?; (vii) what is meant by ‘probability of occurrence’, its relationship with risk, associated dependencies, competing constraints with other risk elements, and behavioral model with respect to time?; (viii) what are probability distribution functions (PDF) and which probabilistic risk distributions are appropriate to risk elements with uncertainty?; (xi) do the axioms of the probability calculus apply to dependent risk elements supporting a single time-dependent risk expression?; (x) how is the quantification of risk measured; what measurement scale is used for risk and CIS (units in: cost, chance of something happening, or lives lost)?; (xi) how can a risk expression for CIS be applied to a risk determination metric?; (xii) what is the relationship between cost and risk?; (xiii) how do environmental enterprise factors affect risk?; (xvi) what are the trade-offs between security countermeasures and mission degradation? It is advantageous, to the principal aim of this content analysis paper, to provide the reader adequate background information that addresses these component questions, as it provides the foundation for a meaningful analysis on the subject of SRA-CIS.

Method of Inquiry

This research paper was a non-experimental, content analysis, of current literature on SRA-CIS. The content within the next few chapters serves to derive and evaluate a continuous, time-dependent risk expression for critical, national information systems, by considering valid, reliable sources of data, and methods supporting quantitative SRA. A Risk Management Framework (RMF) was developed that is centered on the results of this research,

based on a formulated risk determination metric, and relationships identified between independent risk elements.

Existing Federal guidelines, Department of Defense Instructions, policies, and guidance were used to describe and explain the factors that influence risk. Publications from the National Institute of Standards and Technology (NIST) provided information on the Information Risk Management (IRM) of DoD IT systems, specific security risk processes and activities. DoD Instruction 8500.2, IA Department of Defense Information Assurance Certification & Accreditation Process (DIACAP) controls for Classified, Mission Assurance Category (MAC) levels I, II, III were adopted as a vulnerability and control register for CIS.

The adoption, and consolidation of DoDI 8500.2 IA control checklists for MAC I, II, III classified systems, provides vulnerabilities, controls, and system impact data for use in this research paper. The use of fault tree analysis and logic diagrams are methods that represent a forward step in addressing the uncertainty in formulating continuous expressions for risk components. Multivariate analysis was used against a resulting logic table to validate the distinguishable relationships between risk and the fundamental service elements of IA: Confidentiality, Integrity, and Availability (CIA Security Triad). Sensitivity analysis was applied to the proposed risk expressions to identify input elements that have a significant impact. Inputs, which were not thought of as particularly important, can have unexpectedly large effects on the risk output (Rodger, 1999).

A holistic and risk-informed decision-making metric is defined as an analytic tool, for use by Principal Accrediting Authorities (PAA), in the technical approval of a CIS security posture. The determination elements accounted for within this metric include system merits, composite risks, economic analysis, and a risk rate expression for CIS that leverages the

proposed quantitative expression for risk. Determination thresholds for this metric were modeled after unique IA constraints involving CIS currently in operation at United States Pacific Command (USPACOM).

The following work breakdown structure (WBS) outlines the individual research components accomplished in satisfying the objectives of this paper:

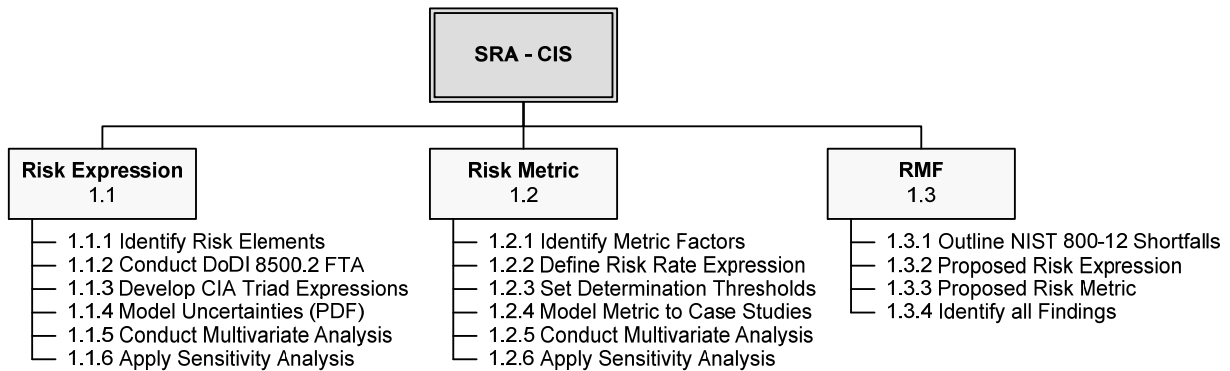


Figure 1. SRA-CIS WBS

Assumptions

Risk is measurable. Uncertainty is not. This paper sought to acknowledge and identify all associated uncertainties with SRA-CIS. As such, the formal expression of risk, as a function of time, requires certain assumptions be made, allowing the modeling of vulnerabilities, threat and frequency contexts to risk. A risk methodology must make some assumption on the future distribution of changes in risk factors. Such methodologies include multivariate normality, multivariate distribution, and historical distribution of changes as a proxy for future distributions (Gibson, 1997).

Limitations

One of the challenges this paper faced was the limited availability of “hard data” regarding many of the important uncertainties in risk analysis. The complicated nature of uncertainty within risk analysis should be captured using models. It is appropriate to adopt Probabilistic Risk Analysis (PRA) techniques, using Probability Distribution Functions (PDF), to represent uncertainties, and to model the growth of exploitable vulnerabilities and corresponding threat conditions. PRA is a quantitative estimate of the consequences and frequency (probability) of an event, including an estimate of the uncertainty given as a statistical distribution (Kastenberg, 1985).

Existing methodological models and the subsequent resulting data arrived from the use of risk expressions, derived from this research paper, is only as accurate as the methods employed and input data used. In other words, ‘you get out what you put in’, such as the saying commonly goes. A certain degree of variability is tolerated, within this research, and is identified, when applicable, during analysis.

Delimitations

Literature related to IS risk mentions numerous risk components and factors that could apply to many different types of situations at different levels (Sherer, 2004). The scope of this paper is confined to risk factors that apply to Critical Information Systems in operation. Limiting the discussion of risk specifically to the operation of CIS creates a gap for the head of an organization responsible for overall organizational risks. However, in the context of CIS operating within a(n) CC/S/A or other DoD enterprise environment, an appointed Designated Approving Authority (DAA), whom is the authorizing official responsible with the decision on

whether to grant an Authority to Operate (ATO) for a CIS, accepts any associated risks in this process, and is the primary stakeholder to benefit from the constraints placed on this analysis.

Paper Organization

This paper is divided into five chapters, where the requirements, details, problems and choices of analytic risk measurement, and determination approaches for SRA-CIS is presented. The results of a comprehensive literature review on risk, within the following chapter, sheds further light on the research questions that have been laid out, additionally elaborating on the fundamental problem behind the purpose of this content analysis study, and the confusion surrounding risk and uncertainty. Chapter 3 identifies the risk elements and components, allowing this paper to formally define risk expressions that make up the quantitative SRA of CIS; further providing methodologies that are used to analyze and validate such expressions within Chapter 4. In the concluding chapter, this paper revisits its results and elaborates on the significance of its general findings.

CHAPTER 2

LITERATURE REVIEW

Purpose of the Chapter

The security of CIS is constantly at risk as new technologies are continuously being introduced into the government sector (Johnson, 2005). By knowing the risks to an organization, theoretically, one can strategically plan to reduce them. SRA is a method that can be utilized, within the risk management process, in identifying present, and even future risks (Elky, 2006). This chapter provides the reader with a review of what is known, and not known, about security risk analysis, security risk assessments, and the confusion surrounding the formal quantification of risk for CIS.

Literature on SRA, as seen within this review, is inundated with countless publications, guidance, policies, procedures, and on-the-fly techniques. Hundreds of articles, instructions, and guidelines identify information system security risks and risk factors, however, the lack of a commonly accepted or underlying theory limits the organizational usefulness of these references (Sherer, 2004). In fact, the subject of SRA-CIS itself is relatively new within the U.S. Government (USG), and thus, should come as no surprise that the majority of literature sources, reviewed by this paper, mainly consist of USG documents and DoD publications. The primary purpose of this chapter is to provide the reader, not only a robust review of supporting literature materials, but an objective viewpoint in which the reader can adopt in arriving at the central problem of this study, namely, the absence of a continuous, time-dependent, quantitative risk expression and corresponding determination metric for CIS.

Organization of the Chapter

The literature review is organized into two general areas of examination, presenting the theory behind adopting Security Risk Analysis (quantitative approaches) versus Security Risk Assessments (qualitative approaches) to CIS. This chapter does not attempt to summarize all the materials published, and referenced in this paper, but instead, synthesizes and evaluates primary key arguments directly pertaining to the research questions outlined within that very section of the introduction.

History of Security Risk Analysis

Risk analysis discussions related to information technology span several decades. Before that, during the Industrial Revolution, steam engines, sparked the first concerns over risks that could be caused by technology (Quantil.com, 2011). Within the DoD alone, the broad subject of risk and the adoption of risk analysis is used for numerous National Security Systems (NSS), with application toward nuclear power reactors, space systems, waste repositories, and incinerators of chemical munitions (Apostolakis, 2004). Information security itself was born out of the practices and procedures of computer security. Recently, the term ‘Information Assurance’ (IA) has been widely adopted, replacing the legacy ‘Information Security’ (InfoSec) term, as the practice of managing risks related to the usage, processing, storage, and transmission of data, information, or information systems (Hansche, 2005).

As technology evolves, the evolution of risk, and risk analysis must also be influenced by our expanding knowledge of threats and vulnerabilities that arise. Integrating and executing proper risk management approaches toward modern CIS – and the decisions that are made in consequence – is paramount, in not only making the most effective use of limited

resources, but also, in facing today's dynamic threat challenges (Quantil.com, 2011).

Problem Breakdown

The subject of risk is both hugely important and horribly elusive. Many rely on 'gut feelings' when presented with situations that require making choices under conditions of uncertainty (Heemstra, 1997). When dealing with national security information it's preferable that officials, at the highest levels of government, do not react from the gut when having to make decisions involving risk, but instead systematically weigh the benefits and harms of such actions. The weighing of potential benefits and harms relies on putting numbers on probabilities; actually quantifying risk and putting it into decisions that are to be made (Harris, 2008). Furthermore, quantitative analysis allows for the development of a standardized risk determination metric, whereby a risk baseline can be compared to an acceptable level of risk, and then used as an aid the decision making process (AIRMIC, 2002).

Risk analysis is considered fully quantitative, if all elements of the process are quantified (asset value, organizational impact, frequency, countermeasure effectiveness, countermeasure costs, probability, and uncertainty). The primary challenge with purely quantitative SRA is that the method attempts to quantify qualitative inputs, and uncertainties inherit within qualitative values. Depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner (NIST SP 800-30, 2002).

A vital component of a proactive security posture is an analysis and understanding of the hazards facing an organization. Security Risk Assessment models, currently employed by CC/S/A, provide for an adequate system security risk snapshot for CIS, but are only

considered a snapshot at the present time (Devost, 2008). The emerging threats to modern CIS and IT infrastructures are real and very dynamic. As such, risk must be treated as a living thing, requiring constant management. The exponential growth of both structured and unstructured threats, acting on existing vulnerabilities against CIS, is alarming and emphasizes the need for a realistic time-dependent risk expression. If IA controls and mitigation measures are not sufficient to counter the increasing rate of threats and vulnerabilities to CIS, then an acceptable risk snapshot that was presented at time, t_1 , may certainly be deemed unacceptable at a future time, t_2 . It is this deficiency, and thus problem, with risk assessment models for CIS that this paper is primarily focused. The author shares the viewpoint that risk analysis must, of necessity, involve different time horizons over which the stability of the system can be investigated (Saaty, 1987).

While a few literary references have recognized risk analysis to be fundamental to the development and operation of IS, none have been able to deliver prescriptive and specific models that principal approving authorities require in making complex risk decisions. The approach taken to the risk analysis itself has largely been based on the use of checklists by analysts in accounting for possible risks. It is possible to make very long lists that are reasonably comprehensive for a particular type of system, however, this approach does not give any confidence that all risks have been identified. It is only when threats and vulnerabilities have been catalogued over time that a risk becomes something very precise and specific. Hence the need for an approach that is complete, consistent and correct. The methodology for SRA should (i) be sufficiently flexible to cope with all CIS models: centralized, decentralized, and distributed systems, and (ii) be both prescriptive and specific, so as to furnish a PAA with real decision-support information. (Birch, 1992).

Quantitative Risk Analysis (QRA) employs two fundamental elements: the probability of an event occurring, and the likely loss, should it occur. In modern risk analysis one needs to determine, numerically, not just what is likely to happen, but also what is important, and what is not important if it does happen. One must consider all observed factors and then establish priorities in the sense of importance and likelihood of occurrence (Saaty, 1987).

In its bare essence, QRA is a top-down approach that follows: (i) a set of undesirable end states (adverse consequences) defined in terms of loss to the mission, the information itself, and to the organization; (ii) for each end state, a set of disturbances or initiating events (IE) to normal operation, is developed whereby, if left uncontained or unmitigated, can lead to the end state; and (iii) event and fault trees, or other logic diagrams, employed to identify sequences of events that start with an IE and terminate at an end state. Accidental scenarios are generated which account for hardware failures, human errors, fires, and natural phenomena. The dependencies among common-cause failures of systems and redundant components receive particular attention. The probabilities of these scenarios are evaluated using all available evidence, primary past experience, and expert judgment. Scenarios are then ranked according to their expected frequency of occurrence (Apostolakis, 2004).

Approximately a-third (1/3) of studies reviewed suggest that risk should be measured as a probability distribution of negative outcomes weighted by financial loss. This tends to show estimates of the probabilities negative outcomes based on statistical techniques or subjective estimates. Sometimes the negative outcomes are converted to monetary terms and expressed as monetary losses in relation to goals and expectations (Sherer, 2004). This paper moves away from the concept of expressing loss as a monetary figure, as CIS deals with information whose sensitivity often does not have an exact assigned dollar value.

Because of the scarcity of reliable data, diversity in the subject matter, lack of a well-established methodology, and the unavoidable degree of subjectivity of data, a resulting quantitative risk analysis proves to be a difficult thing to accomplish (Elky, 2006). Many risk scholars have, gone as far as to, question the possibility of even conducting an objective analyses of risk; whether technical risk estimates represent “objective” probabilities of harm. Furthermore, they question if QRA results should be given any consideration when a high degree of uncertainty is inherited (Klinke, 2002).

Common criticism exist, in that probabilities, flat out, cannot be realistically calculated (Apostolakis, 2004). It is the position of this paper that these uncertainties exist independently of whether QRA is used or not, and decisions to be made regarding CIS, are better made if quantitative information is available. By attempting to quantify the uncertainties and identify dominant risk contributors, QRA contributes to the common understanding of the issues and, in addition, may provide useful input in the allocation of IT resources (Klinke, 2002).

It is important to note that QRA is performed for systems that are highly reliable and well-defended, thus, a plethora of failures does not exist, which would be considered highly undesirable to begin with. As indicated earlier, every decision involves at least some element of uncertainty, however, in some risk classes, the effects of uncertainty are so small that they can be ignored for purposes of analysis (Jedamus, 1969). This isn't to say that QRA methods do not analyze rare events. In fact, a systematic approach can certainly be adopted that takes advantage of all available information in evaluating probabilities. Those adopting QRA must be fully aware of the extensive use of expert judgment and the factoring of uncertainties associated with the results. Ultimately, one must understand that the decision making process itself is considered to be risk-informed and not risk-based (Apostolakis, 2004).

In dealing with the subject of uncertainty, an argument is commonly raised that, analytical methods lose their usefulness in situations where the amount of data available is insufficient, and where uncertainties are considered too great. “You can’t use fancy methods if you haven’t got the numbers to put in” is the way the argument usually goes. Even so, it must be held that, the greater the number of uncertainties faced, is more of a case, and need, for an analytical structure (Jedamus, 1969).

While formulas and techniques are important, they should be understood for what they are: a means of transition between a nonmathematical process of applied logic and solutions to practical problems in applied decision making. More importantly, to create a mathematical model that exactly describes all the variables and interrelationships, for all CIS, even for a small part of such a system, is extremely complex (Jedamus, 1969).

An objective point of view considers probability as the ratio of successful outcomes of an experiment to the total number of outcomes possible, or as the “relative frequency” of successful outcomes. According to this subjective view, a probability is simply a number representing a degree of belief concerning the occurrence of a future event (Kyburg, 1970). The only limitation regarding this number is that it be between zero and unity. Complete certainty that a particular event will occur is equated with the probability of one (1). Complete certainty that the event will not occur is equated with a probability of zero (0). Less than complete certainty concerning the event must then be characterized by a probability somewhere between 0 and 1 as shown in Figure 2 below.

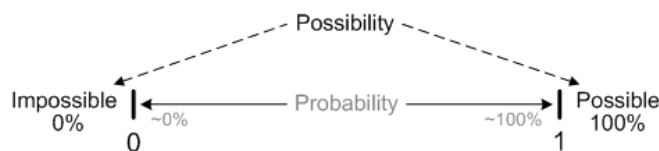


Figure 2. Probability Bounds (Jones, 2008)

The concept of probability bounds becomes of great importance in Chapter 3 when establishing the numerical bounds of a risk model. Ultimately, it is taken that objective and subjective probabilities are not contradictory. From the perspective of the decision maker either viewpoint may be adopted (Jedamus, 1969).

There are risk elements whose contributions or influence are not probabilistic. Given a set of factors, one can ask which of them has a greater influence on the outcome, or which one has the higher priority influence. This lack of complete representation has been a serious flaw in risk analysis where everything is described in terms of probabilities alone (Saaty, 1987). When dealing with independent factors there needs to be a way to represent such interactions and dependencies holistically in our structures for handling risk. This is an important concept that is preserved in Chapter 3 when modeling a quantitative risk expression that involves probabilities.

Literature addressing a formal time-dependent risk determination metric is scarce at best. The traditional approach, in being able to address the second research question (RQ2) of this paper, appears to be the disposition of an organization to risk, based on the concept of the utility function, and the rate of change of its second derivative with respect to the first derivative (Saaty, 1987). The calculation of the utility function involves the probability of risk. Such a method is adopted, further detailed within the following chapter on methodology, and henceforth referred to within this paper as a 'risk rate'.

Qualitative Risk Assessment is the most widely used approach to risk analysis. Probability data is not required for such assessments and only estimated potential loss is used. Qualitative risk assessments assume that there is already a great degree of uncertainty inherent within the likelihood and impact values; defining them, and thus risk, in somewhat subjective

or qualitative terms. Similar issues are seen in QRA, with difficulty in defining the likelihood and impact values. Moreover, these values need to be defined in a manner that allows the same scales to be consistently used across multiple risk assessments (Elky, 2006).

The results of qualitative risk assessments are inherently more difficult to concisely communicate to management. Qualitative risk assessments typically give result ratings of “High”, “Moderate”, and “Low”. However, it is only by providing the impact likelihood definition tables, and a description of the impact, does it become possible to then communicate such an assessment (Elky, 2006).

A quantitative risk assessment, not to be confused with quantitative risk analysis, draws upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, processes, recovery costs, etc., impact - risk, can therefore be measured in terms of direct and indirect costs (Elky, 2006). An Annualized Loss Expectancy (ALE) value is often used to express the monetary loss that can be expected for an asset due to a risk over a one year period. It is defined as:

$$ALE = SLE \times ARO \quad (1)$$

where, Single Loss Expectancy (SLE) is the dollar amount (asset value) assigned to a single event that could be lost given the organizations potential loss amount (exposure factor, EF), if a specific threat agent exploiting a vulnerability were to take place:

$$SLE = \text{asset value} \times EF \quad (2)$$

, and where the Annual Risk Occurrence (ARO) represents the estimated frequency of a specific threat taking place within a one-year timeframe (Harris, 2008). The safeguard value or benefit analysis to the organization becomes:

$$(ALE \text{ without safeguard}) - (ALE \text{ with safeguard}) - (\text{annual cost of safeguard}) \quad (3)$$

The determination metric for the implementation of a countermeasure is simply expressed as a cost inequality where if:

$$\text{countermeasure costs} < \text{potential loss} \quad (4)$$

then a decision to implement such a countermeasure will be cost beneficial to the organization in the long term.

While utilizing quantitative risk assessments seems straightforward and logical, there are issues using this approach towards CIS. While the cost of a system may be easy to define, the indirect costs, such as value of information, loss of production activity, and the costs associated with recovery is imperfectly known at best. The other major element of risk, *likelihood*, is often even less perfectly known. For example, what is the likelihood that someone will use social engineering to gain access to a user account on a CIS (Elky, 2006)?

Review

Risk carries many different meanings with many formal methods used to assess and "measure" risk. Risk to CIS is a function of the likelihood of a given threat source exercising a particular potential vulnerability, with the resulting impact of that adverse event taking on a loss for the organization. The uncertainties in risk can be quantified using probabilities based on past data and experience, however, it is crucial that the specific scope and limitations of this paper be kept in mind when methodically deriving a formal expression, and risk-decision metric for CIS.

A large margin of error is typically inherent in QRA for CIS. This may not always be the case in the future, as the body of statistical evidence becomes more widely available, and where trends can be extrapolated on past experience. If the information is deemed reliable, a

qualitative risk analysis is an extremely powerful tool to communicate risk to management (Elky, 2006).

Summary

Several key issues regarding the quantification of risk have been presented in this chapter. The general conclusion from this literature review is that most materials on risk theory are a jumble of diverse models, and partially overlapping, theoretical lists of risk factors and risk components. The research, and corresponding component, questions developed, in Chapter 1, for this study has allowed this paper to filter and focus in on the nature of risks and risk factors that directly apply to SRA-CIS. Heading into the following chapter, focus will shift to methodologies that will formally put the supporting information covered in this literature review together, arriving at meaningful relationships for analysis that will accomplish the tasks set out within the WBS and, ultimately, satisfying the purpose of this study.

CHAPTER 3

METHODOLOGY

Purpose of the Chapter

To its reader the methodology, outlined in this chapter, represents a significant step forward in the comprehension and knowledge of SRA-CIS. The purpose of this chapter is to provide a methodology upon which a unique, quantitative, definition of a continuous, conditional risk expression (WBS 1.1), and corresponding risk determination metric (WBS 1.2) for CIS that, can be thoroughly examined and subjected to applicable analysis methods. This chapter outlines the techniques and models used to approach the main problem of this content study, addressing both the research and subsequent questions in Chapter 2, namely, (i) the absence and possibility of a truly quantitative risk expression and blanket risk decision metric for CIS, and (ii) whether such expressions for SRA is applicable and meaningful within the field of CIS - an application surrounded by uncertainty.

Organization of the Chapter

This chapter is organized into three major areas where (i) the reasoning and techniques that are directly relevant in arriving at WBS 1.1 and WBS 1.2, are presented; (ii) probabilistic estimates for the quantitative models of this paper, including the methods, for existing qualitative frameworks, and required parameters / constraints to establish a meaningful comparison between the results of these models are presented; finally, (iii) formal procedures and analysis methods are outlined for the validation of presented models.

A bottom-up approach is taken in concert with a systematic and comprehensive

methodology in helping identify the key variables, and combination thereof, which influence risk. The methods employed in analyzing risk element relationships focus on (i) vulnerabilities inherent within CIS, (ii) threats to the CIA of CIS, (iii) controls & measures used for protection, (iv) resulting consequence and associated impact magnitude to the organization. The aggregate focus of all sections within the chapter is directed at the formal establishment of both time-independent, and time-dependent quantitative models, for SRA-CIS, with appropriate validation procedures in comparing quantitative results to existing qualitative models adopted by CC/S/A (specifically by USPACOM).

Method of Inquiry

Technique

In order to lay a meaningful foundation for the methodological exploration of SRA-CIS, the study began by first identifying, discussing, and defining the relevant factors wherein the context of this study is centered on: Risk (WBS 1.1.1). This approach begins by asking: *What is risk?* Literature on the subject reveals many inconsistent and ambiguous meanings, adding confusion to an already complicated topic. There are many kinds of risk that can be extracted from a wide range of unique fields. The term itself is found to be used in many different senses and, in the case of information systems security, is often used very loosely (Kaplan, 1981).

Webster's dictionary offers a simple binary definition, that is, risk as the 'possibility of loss.' The International Organization for Standardization (ISO) defines risk as the 'effect of uncertainty on objectives' (ISO 31000, 2008). Both definitions, although wonderfully encompassing and yet very much abbreviated, must be elaborated further for our purposes. The term 'effect', as identified by the ISO, is more commonly referred to as *impact* or

consequence, and may be both negative and positive impacts on objectives. This is supported by the Project Management Institute (PMI), Project Management Body of Knowledge (PMBOK), an international standard, in which risk is defined as having both ‘a positive or negative influence’ (PMBOK, 2004). Depending on an individual stakeholder’s viewpoint, a risk may, in fact, be considered an ‘opportunity’ if the resulting impact were favored as positive. For example, in the case of financial risk, the unexpected variability or volatility of returns includes both potential worse-than-expected, as well as, better-than-expected returns (Jorion, 2006). From this point forward, and in respect to information security risks, any reference to risk should be considered as having a negative impact (loss) unless the context precludes this interpretation. Note that risk is the negative (complement) of opportunity:

$$\text{Risk} = -\text{Opportunity} \quad (5)$$

The issue of ‘uncertainty’ is one of the major topics of debate in the risk community. The word itself is often used without formal definition. The concept of uncertainty refers to the degree to which one lacks confidence in an estimate and is expressed as a percentage from 0 to 100 percent (Bell, 1999):

$$\text{Uncertainty} = 100\% - \text{confidence} \quad (6)$$

The term refers to events which may or may not happen, and includes uncertainties resulting from ambiguity or lack of knowledge. Philosophers of risk have asserted that the term often implies a portfolio of different aspects that are often neglected or amalgamated in risk analysis (Klinke, 2002). Although this may be case, uncertainty should not infer negative connotations. In fact, several aspects, out of the numerous uncertainties associated with information system-related security risks, can be ruled out or eliminated based on the negligible effect or impact those aspects could have.

In the case of SRA-CIS, uncertainty analysis is utilized (Chapter 4) with the notion that probability can be used to quantify degrees of certainty or uncertainty: (e.g. a higher probability can be used to express a higher degree of certainty that something will, in fact, happen). The first component to this analysis includes the identification and justification of probabilities linked to specific adverse events or distribution of effects. The term “probability of occurrence” is adopted within risk theory for events for which data exists on past trends, information about cyclical events, logical inferences from systematic observations, or beliefs based on institutional experience. These data sources form the building blocks for estimating the relative frequency of an adverse effect over time.

From the initial definitions presented for perceived risk it becomes possible to arrive at the following general expression:

$$\text{Risk} = f_{\text{impact}}(\text{uncertainty}) \quad (7)$$

Adopting the interpretation that risk is associated with consequences that involve losses to the risk taker (Rowe, 1975), in conjunction with the concept of uncertainty in (6), yields the following:

$$\text{Risk} = -|f_{\text{impact}}(100\% - \text{confidence})| = \text{loss} \quad (8)$$

According to NIST special publication (SP) 800-53, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) the adverse impact, ω_i that would arise if indexed event, i , occurs; and (ii) the likelihood (probability) of occurrence, $P(i)$, thus

$$\text{Risk} = f(\text{impact, probability}) = f[\omega_i, P(i)] \quad (9)$$

In this regard, it is of interest to note that, although both the negative value of impact and value

assignment for the probability of occurrence are measurable, they are not necessarily independent as implied by (5). Even so, this paper examines the common approach to expressing risk, namely, the Bayesian concept of expected value, whereby the product of the probability and consequence values are summed to provide an expected value of the risk being undertaken (Rowe, 1975). For an adverse indexed event, i , with n possible consequences, the expected value (EV) of risk can be expressed as:

$$\text{Risk}_{EV} = \sum_n \omega_{i,n} \cdot P(i) \quad (10)$$

The definition of risk has widely been characterized, especially in the insurance industry, not by ‘what it is’, but instead by the properties with which it has (Buhlmann, 2005). Thus, in the thorough pursuit on the proper definition for risk, focus is shifted to understanding: *What are the properties (variables and elements) of risk?* We begin with NIST SP 800-30, and risk as ‘the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence’ (NIST SP 800-30, 2002). This states that a risk exists when a vulnerability and corresponding threat overlap. That is, there is a threat and a vulnerability, which may be exploited, to realize that threat. An attempt to exploit a risk – to realize a threat – is called an attack and is considered an adverse event (Harris, 2008). Risk is relative to the observer (Kaplan, 1981), however, a common error in uncertainty and risk analysis is to double count the risks (Rodger, 1999). Note that the same attack may be attempted by different attackers: in each case, this constitutes a separate risk (Birch, 1992). Following identification of these risk variables for CIS, the risk definition in (9) is now amended to read as:

$$\text{Risk} = f \left[\text{impact, probability}(\text{vulnerability} \mid \text{threat}) \right] \quad (11)$$

$$= f[\omega_i, P_i(\lambda_i|\theta_i)] \quad (12)$$

The EV in (10) is also amended to include the conditional probability of vulnerability, λ , given a threat, θ , as:

$$\text{Risk}_{EV} = \sum_n \omega_{i,n} \cdot P_i(\lambda_i|\theta_i) \quad (13)$$

where

$$\neq \sum_n \omega_{i,n} \cdot P_i(\lambda_i) \cdot P_i(\theta_i) \quad (14)$$

, such that,

$$0 \leq P_i(\lambda_i|\theta_i) \leq 1 \quad (15)$$

$$0 \leq P_i(\lambda_i) \leq P_i(\theta_i) \leq 1 \quad (16)$$

The expression arrived in (14) is a source of contention in modern SRA for CIS and is commonly encountered (Jones, 2008) as:

$$\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact} \quad (17)$$

It is argued that the expected value in (14) and (17) is misleading, violating the axioms of probability calculus, as it (i) fails to take into account all potential outcomes – both positive and negative consequences, and (ii) implies that the vulnerability and threat variables are independent of each other.

Although the argument in (i) is true for general risk, it is the position of this paper that, the interpretation adopted in (8), regarding the relativity of risk, can be applied to (13), by uniquely defining an event space or universal set, U , for risk, that consists of the sum total of n , potential occurring and non-occurring, events that specifically result in a loss. Thus, an event, E_i , where i indicates an event index, is determined by its description, D_i , and

probability of occurrence, P_i , (Rowe, 1977) as:

$$E_i = [D_i, P_i] \quad (18)$$

and

$$U = \sum_{i=1}^n (E_i + \bar{E}_i) = \sum_{i=1}^n \{ [D_i, P_i] + [\bar{D}_i, (1 - P_i)] \} \quad (19)$$

To reiterate, (19) provides for the model definition of a limited universe whereby numerous events resulting in little to no impact upon risk may be omitted in the interest of a pragmatic simplification of a potentially exhaustive and collective analysis.

The argument in (ii), is best supported by understanding: *What are vulnerabilities and its constraints with threats?* A vulnerability is a weakness that can be exploited. In the case of CIS, vulnerabilities are a characteristic property of the physical implementation of the IS and are independent from any threats to the IS (Birch, 1992). This is not to be confused, with the fact that the *exploit probability* of a vulnerability is dependent and, in fact, conditional based on the occurrence of a threat potential, resulting in an attack against a CIS. Note that vulnerabilities, however, are not merely flaws in the physical implementation provided by the system, but may extend to include breaches and violations at the policy level (Elky, 2006).

Vulnerabilities for CIS vary depending on the boundary and environment with which a CIS operates in. Theoretically, the number of vulnerabilities at any particular point in time is finite, however, is not attainable in actual practice given the technical security complexities of modern CIS. (i.e. zero day exploits - vulnerabilities that are unknown and have no fix or patch at the time of exploitation). Additionally, vulnerabilities are on the rise. The combination of increased vulnerabilities and an ever-growing amount of confidential data presents a unique and individual threat to information assets. The frequency of occurrence for the exploitation

of any particular vulnerability is actually a very complex function. This function depends on such elements as the gain to the attackers, the cost of the attack, the chance of detection, etc. (Birch, 1992).

Vulnerability analysis is used to catalogue known vulnerabilities of a system, assigning a probability value for the vulnerability being exploited in a given time. The number and diversity of vulnerabilities that need to be covered is the factor which causes the most problems. To assist in dealing with vulnerabilities, it is worth developing a broad classification of vulnerabilities as adopted within Table 3 of the “Data” section of this chapter.

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A threat-source does not present a risk when there is no vulnerability (NIST SP 800-30, 2002). In today’s threat environment, a threat assessment methodology is a vital component of an organization’s security program. This methodology should account for a wide variety of threats, and should be based on realistic threat information projecting future threats, while also accounting for previous experiences, incidents, and documented attacks within an organizations’ peer group (Devost, 2008).

Threat analysis consists of cataloging each and every threat to the organization. In the case of CIS, this means cataloguing threats to information assets on the information model. For every information asset on the information model, three threats are catalogued: the Confidentiality (C), Integrity (I), and Availability (A) threats (Birch, 1992).

Controls are implementations that (i) prevent any initial exposure to a threat, (ii) detect if a threat has been realized against the system, (iii) mitigate the impact of a threat against the system, and (iv) recover/restore the system (Meritt, 1999). Security controls for CIS encompass the use of both technical and non-technical methods, each of which can be

subcategorized into either preventive or detective controls. When dealing with the security of CIS, and the implementation of controls, an information centric approach is usually adopted.

Information centricity is important because it provides a holistic view of potential security incidents across an entire distributed infrastructure (DoDAF, 2009). Following the path of data communications will show where the potential for risk exists between endpoints. Ensuring the protection of data in transit, at rest on a fileserver, and its use by applications, are accomplished using encryption, key management, data loss prevention techniques, and logs to help monitor and report malicious activities. Activities detected that fall outside of policy that are deemed unusual, may be an indication of fraud.

Information Assurance (IA) differs from information security, operationally, in that additional emphasis is placed on information sharing and the mechanisms for establishing and controlling trust amongst users through authorization and authentication (Cieslak, 2009). The US PACOM Information Services Reference Model describes the Information Assurance Services as 'the ability to protect and assure information and info structure' within seven categories based upon the revised Defense-in-Depth vision (Cieslak, 2011). The symbol, s , is designated as the IA services index, with each of the categories listed within Table 3, in black.

Information system-related security risks are defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization". These risks arise from the loss of the following Information Security Services (ISS): Confidentiality, Integrity, and Availability (CIA) of information or information systems (NIST SP 800-53, 2010). These individual services are constrained together, within a triad, as shown in Figure 3. The main concept behind the triad model is that, as one moves closer to the toward the apex of a service, the further one moves away from the other two services (i.e.

the more one makes information available, the less confidential it becomes). The idea is to make the tradeoff a sensible one (Kinamik, 2007) by balancing a central mixture of services.

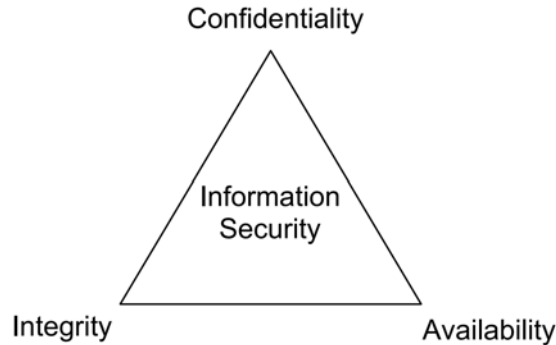


Figure 3. CIA Information Security Triad (Harris, 2008)

This relationship takes on more relevance in Chapter 4, as the CIA IAS is closely examined with its adoption, by this paper, as the primary unit of measure (risk dimension) for all quantitative models. We express the constraint by the model simply as:

$$\text{Information Security} = \text{CONF} + \text{INT} + \text{AVAIL} \quad (20)$$

Expressions in (9) and (11) are elaborated further to read:

$$\text{Risk} = f \left[\text{impact}(\text{CIA Services}, \text{CAT Rating}, \text{MAC}, \text{costs}), \text{probability} \right] \quad (21)$$

$$= f \left[\omega_i(\text{CONF}, \text{INT}, \text{AVAIL}, \omega_{\text{CAT}}), P_i(\lambda_i | \theta_i) \right] \quad (22)$$

Countermeasures are applied to reduce exposure to risk. Depending on the nature of the risk, an organization may choose from a range of countermeasures, categorized as (i) risk shifting, where risk itself moves all or part of the exposure to a third party, (ii) risk reduction, where the exposure is reduced because a control is applied to the vulnerability which reduces the frequency of occurrence and, (iii) risk avoidance, where a countermeasure is applied to reduce the impact of the threat (Birch, 2001). The execution of countermeasures can *increase* confidence, and from (8) thereby *reduce* risk, within a particular IAS.

The confidence factor, $\gamma_{s,n}$, is formally reintroduced as a risk element having a direct effect on risk, bounded by unity [0,1], and interpreted as:

$$\omega_{s,n} \cdot (1 - \gamma_{s,n}) \quad (23)$$

Implementation of DIACAP IA controls as countermeasures for individual system vulnerabilities listed within DoDI 8500.2 are designated by a compliant (C), non-compliant (NC), or not applicable (N/A) evaluation. An Information Assurance Officer (IAO) tasked with the responsibility of maintaining compliance with the implementation of these controls can effectively minimize and/or eliminate the probability of a threat exercise of a system vulnerability (NIST SP 800-30, 2002). The effect of a control, $\delta_{s,i}$, against the conditional ‘probability of an attack’,

$$P_{s,i}(\lambda_{s,i} | \theta_{s,i}) = \frac{P(\lambda_{s,i} \cap \theta_{s,i})}{P(\lambda_{s,i})} = \frac{n(\lambda_{s,i} \cdot \theta_{s,i})}{n(\theta_{s,i})} \quad (24)$$

, is expressed as the ‘effectiveness of the control’ (Sandia, 2006) as,

$$1 - \delta_{s,i} \quad (25)$$

where,

$$\delta_{s,i} = \begin{cases} 0, & \text{iff Non-Compliant (NC)} \\ 1, & \text{if Compliant (C) } \oplus \text{ Not Applicable (N/A)} \end{cases} \quad (26)$$

From (13), (15), and (16) the likelihood of a successful attack, against a mitigated vulnerability through the implementation of a control, then becomes:

$$P_{s,i}(\lambda_{s,i} | \theta_{s,i}) \cdot (1 - \delta_{s,i}) \quad (27)$$

Impact refers to the magnitude of harm caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for CIS affected (NIST SP 800-30). It's not possible to define a generalized impact metric because the nature of impact varies from organization to organization (Birch, 2001). It is possible, however, to define an impact metric for DoD organizations, operating a CIS, based on Mission Assurance Categories (MAC), severity categories of controls, and the classification of data involved.

The subject of impact involves the question of how to measure the quantification of risk and the methodology behind establishing a relative value measurement scale (risk dimension). The methodology, followed by this paper, for a risk unit of measure goes back to the core principles of information security, namely, the IAS: Confidentiality, Integrity, and Availability (CIA) security triad (WBS 1.2.1). The bounds of this measurement dimension is unity (0,1] and can be factored interchangeably with the other risk dimensions following (20).

By preserving the unity bounds of both the risk dimension and individual risk elements, the cumulative product of N risks is made possible:

$$\text{Risk}_{EV} = \prod_i^N R_i \quad (28)$$

where

$$\lim_{N \rightarrow \infty} \text{Risk}_{EV} \simeq 0 \quad (29)$$

and 'risk is never zero' (Kaplan, 1981):

$$\text{Risk} \neq 0 \quad (30)$$

The meaningful interpretation of this unit of measurement is further elaborated, within the descriptive statistics section, of the analysis chapter.

Severity Categories (CAT) are assigned to a system security weakness to indicate the risk level associated with the security weakness and the urgency with which corrective action must be completed (DoDI 8510.01, 2007). A mapping of severity categories with associated security vulnerabilities are listed within Table 3 of the “Data” section of this chapter. The impact factor to a non-compliant control, for the qualitative assessment of a CIS at USPACOM, is a 3-point percentage, confidence (IAS.CONF_s) degradation calculation within the Information Assurance Service (IAS), *s*, in which the control belongs to.

Table 1

DoDI 8510.01 Severity Categories and associated USPACOM Impact Factors

CAT ω_{CAT}	DESCRIPTION	IMPACT FACTOR $\omega_{s,i}$
1	Findings that allow primary security protections to be bypassed.	IAS.CONF _s - 40%
2	Findings that have a potential to lead to unauthorized system access or activity.	IAS.CONF _s - 10%
3	Findings that may impact IA posture but are not required to be mitigated or corrected for an ATO.	IAS.CONF _s - 5%

The quantitative model adopted within this content study maps severity categories, ω_{CAT} , directly to impact factors, $\omega_{s,i}$, while adopting the same qualitative 3-point degradation model used by USPACOM Certification & Accreditation (C&A) analysts. Calculating a 3-point quadratic regression, the impact factor for quantitative analysis becomes:

$$\omega_{s,i} = \frac{1}{100} \left(1 - \left| -12.5\omega_{CAT}^2 + 67.5\omega_{CAT} - 95 \right| \right) \tag{31}$$

However, instead of subtracting the impact factor from the confidence of an IA security service group, the impact factor becomes a multiplicative product with risk.

From the comprehensive completion of WBS 1.1.1, the proposed risk logic diagram, in Figure 4, provides a basic illustration for the condition of relative risk given the set of risk variables, Ω , and a unique universal set, U , as identified in Chapter 2.

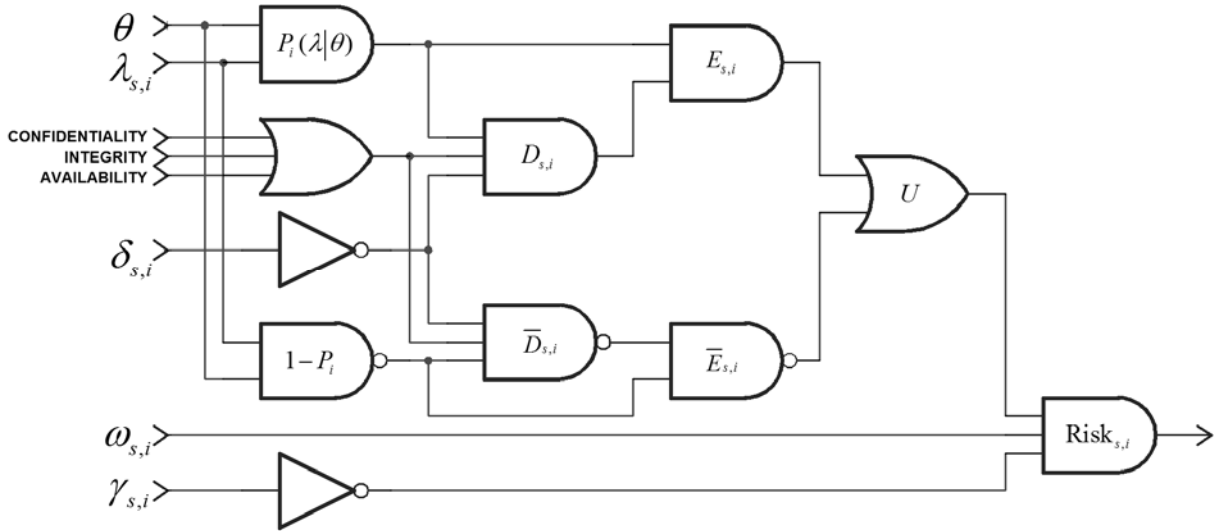


Figure 4. Risk Logic Diagram for CIS (WBS 1.1.2)

The resulting Boolean operation is an expression that can be used in the simple case of a binary possibility (incident or no incident), risk is then:

$$\text{Risk}_i(\Omega) = \neg\gamma \wedge \omega \wedge U \quad (32)$$

$$= \neg\gamma \wedge \omega \wedge (\neg E \vee E) \quad (33)$$

and considering the relativity of risk for CIS:

$$\text{Risk}_i(\Omega) = \neg\gamma \wedge \omega \wedge E \quad (34)$$

$$= \neg\gamma \wedge \omega \wedge (D \wedge P_i) \quad (35)$$

$$= \neg\gamma \wedge \omega \wedge [\neg\delta \wedge (\text{CONF} \vee \text{INT} \vee \text{AVAIL}) \wedge (\theta \wedge \lambda)] \wedge (\theta \wedge \lambda) \quad (36)$$

$$= \neg\gamma \wedge \omega \wedge [\neg\delta \wedge (\text{CONF} \vee \text{INT} \vee \text{AVAIL}) \wedge \theta \wedge \lambda] \quad (37)$$

$$= \theta \wedge \lambda \wedge \neg\delta \wedge \omega \wedge \neg\gamma \wedge (\text{CONF} \vee \text{INT} \vee \text{AVAIL}) \quad (38)$$

On the proposed, formal, *time-independent*, quantitative risk expression for CIS, let the set of indexed risk elements, Ω_i , be defined as threats, vulnerabilities, controls, impact, confidence, and unique universal set, or

$$\Omega_i = \{\langle \theta_i, \lambda_i, \delta_i, \omega_i, \gamma_i, U \rangle\} \quad (39)$$

respectively, where risk element $i = 1, 2, 3, \dots, N$ and probability, P_i , where $(0 \leq P_i < 1)$, and from (27):

$$\text{Risk}_{EV}(\Omega_i) = \prod_{n=1}^A \sum_{s=1}^B \sum_{i=1}^{C(s)} \{1 - [P_{s,i}(\lambda_{s,i} | \theta_{s,i}) \cdot (1 - \delta_{s,i})] \cdot [(\omega_{s,n}) \cdot (1 - \gamma_{s,n})]\} \quad (40)$$

where (15), (16), (26), and:

$$A = \begin{cases} 1, \text{ Confidence (CONF)} \\ 2, \text{ Integrity (INT)} \\ 3, \text{ Availability (AVAIL)} \end{cases} \quad B = \begin{cases} 1, \text{ Physical Security} \\ 2, \text{ Cyber Security} \\ 3, \text{ Continuity} \\ 4, \text{ Security Design} \\ 5, \text{ Security Education} \\ 6, \text{ Identity A\&A} \\ 7, \text{ Content Security} \end{cases} \quad C(s) = \begin{cases} 23 \text{ iff } s = 1, \\ 35 \text{ iff } s = 2, \\ 17 \text{ iff } s = 3, \\ 39 \text{ iff } s = 4, \\ 6 \text{ iff } s = 5, \\ 18 \text{ iff } s = 6, \\ 4 \text{ iff } s = 7 \end{cases} \quad (41)$$

As risks concerned with the operation of CIS is fundamentally about uncertainty during a time interval, the proposed formal *time-dependent* (continuous), quantitative, conditional probability risk distribution function, R , bounded by unity (0, 1], is formally defined and based on the quantitative, EV model in (40):

$$R_n(t) = \int_U \{1 - \{P[\lambda(t) | \theta(t)] \cdot [1 - \delta(t)]\} \cdot \{\omega \cdot [1 - \gamma(\delta, t)]\}\} dt \quad (42)$$

$$= dt \Big|_U - \int_U \omega \cdot P[\lambda(t) | \theta(t)] \cdot [1 - \delta(t)] \cdot [1 - \gamma(\delta, t)] dt \quad (43)$$

The introduction of time dependence for a CIS risk expression allows behavioral elements associated with the forecast of risk itself, not previously witnessed with non-time dependent qualitative and quantitative expressions, to be appended into the original risk expression to create a corresponding risk determination metric that can now take into account both the rate of risk and risk variability. Although it may seem that the behavior of risk would appear to be an element of risk itself, there is hesitation to modify the risk expression in (43) to recursively define risk as a product function of the rate of changes of itself, to include (i) its second derivative and, (ii) its first derivative with respect to itself. Instead the unique function is treated as a risk determination expression such that:

$$\text{Risk Determination} = \text{Risk} \times \text{Risk Rate} \times \text{Risk Rate Variance} \quad (44)$$

or

$$D(R) = R \cdot R' \cdot R'' \quad (45)$$

However, in the interest of keeping the determination metric, D , bounded by unity (0, 1], the first and second derivatives are each individually fed into modified arctangent functions bounded (-1, 1) by dividing the trigonometric function by the asymptotic value of $\pi/2$. Both resulting functions are summed by unity, and with (45), can be meaningfully expressed as:

$$D^*(R) = R \cdot \left[1 + \frac{2}{\pi} \tan^{-1} \left(\frac{dR}{dt} \right) \right] \left[1 + \frac{2}{\pi} \tan^{-1} \left(\frac{d^2R}{dt^2} \right) \right] \quad (46)$$

The DAA is responsible for determining whether a risk is at an acceptable level, or whether additional security controls should be implemented to further reduce or eliminate any residual risks, before accrediting and issuing an ATO for a CIS. We understand risk evaluation as the process by which agencies determine the acceptability of a given risk (Klinke, 2002). It is the position of this paper that the output values from the determination

metric in (46), for each ISS risk dimension (CIA), are to be compared to the CIS Mission Assurance Category (MAC) to arrive at an appropriate risk decision. MAC’s are primarily used to determine the requirements for availability and integrity (ISSDD, 2010). There are three qualitative Mission Assurance Categories, each with consequences to the mission, defined by IAS thresholds. Note, however, that 8500.2 MAC levels do not specifically define confidentiality thresholds. MAC assignments are associated in terms of the adopted unit of measure for qualitative measurement (risk dimension) as in Table 2 below:

Table 2

MAC and Required Associated Risk Dimensions for Risk Determination Metric

MAC	DESCRIPTION	RISK DIMENSION, $R_{s,n}$
I	Consequences of loss of INT or AVAIL are unacceptable.	$R_{s,2}, R_{s,3} \geq 0.70$
II	Consequences of loss of INT is unacceptable. Loss of AVAIL is difficult to deal with.	$R_{s,2} \geq 0.70$ $R_{s,3} \geq 0.75$
III	Consequences of loss of INT or AVAIL is tolerable.	$R_{s,2}, R_{s,3} \geq 0.60$

A risk methodology must make some assumption on the future distribution of changes in risk factors. Such methodologies include multivariate normality, multivariate distribution, and historical distribution of changes as a proxy for future distribution (Gibson, 1997).

Models are guides. They can be out-of-date, wrong, simple, or too complicated, but overall they can be useful. Without a formal assessment methodology to model uncertainties such as vulnerabilities and threats, a time-dependent, quantitative, probability distribution function becomes difficult to express. This includes modeling threats and vulnerabilities to probability of occurrence functions or PDFs (WBS 1.1.4).

For this study, the independent PDF adopted for vulnerabilities within this quantitative analysis is a quadratic regression of 2006 data from the United States Computer Emergency Readiness Team (US-CERT) database. The data points have been plotted and curve fitted in Figure 5.

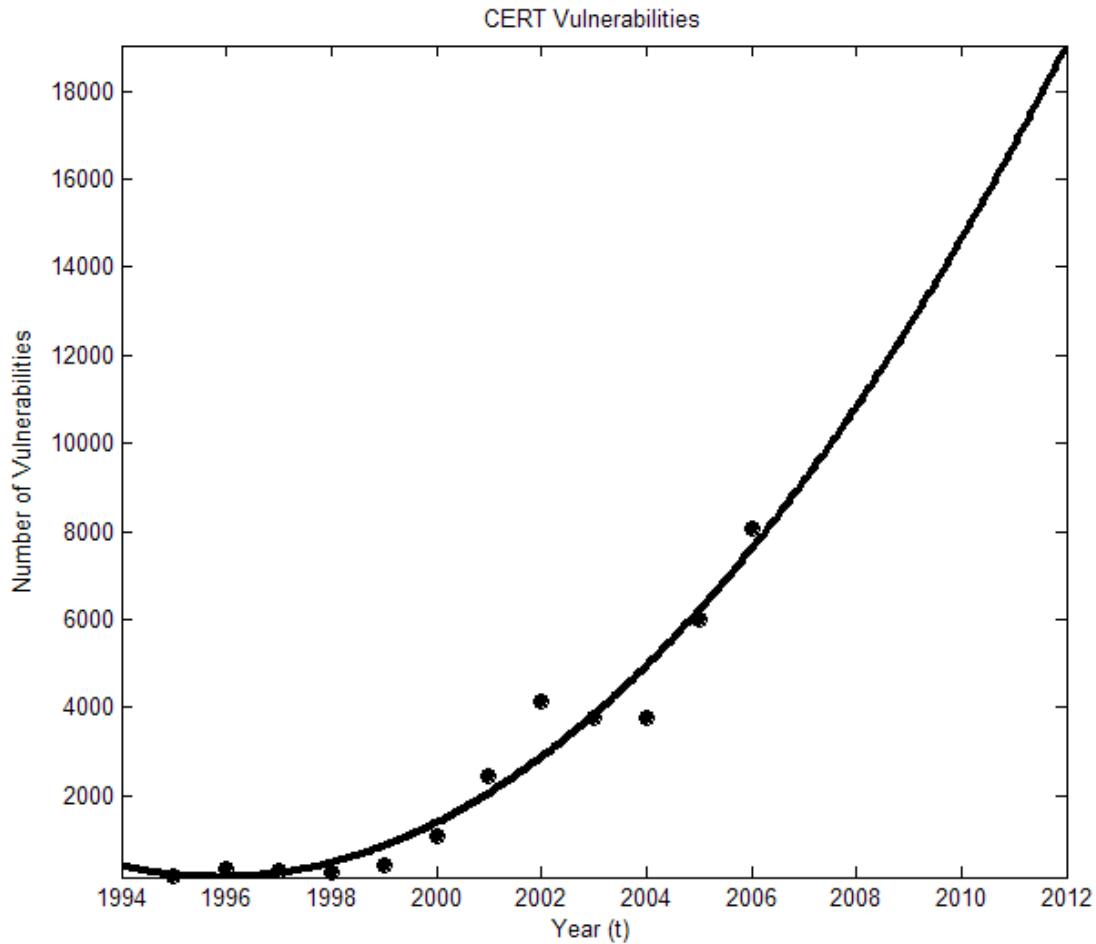


Figure 5. US-CERT Vulnerability Plot

The quadratic regression plot in Figure 5, for vulnerabilities, $\lambda(t)$, represents an increasing probability of occurrence function with respect to time:

$$\lambda(t) = (73)t^2 - (2.9 \cdot 10^5)t + (2.9 \cdot 10^8) \quad (47)$$

The independent PDF adopted for threats within this quantitative analysis is a quadratic regression of 2007 data from the United States Computer Emergency Readiness Team (US-CERT) database. The data points have been plotted and curve fitted in Figure 6.

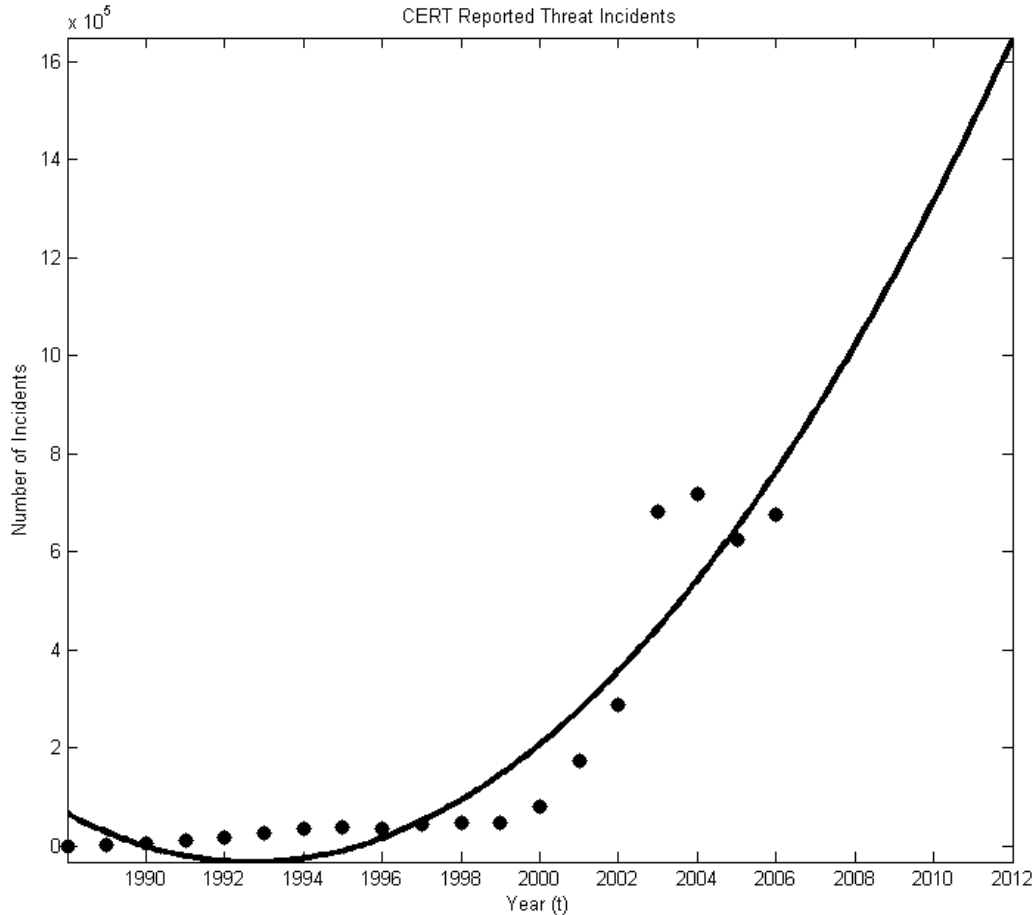


Figure 6. US-CERT Threat Incident Plot

The quadratic regression plot in Figure 6, for threats, $\theta(t)$, represents an increasing probability of occurrence function with respect to time:

$$\theta(t) = (4.5 \cdot 10^3)t^2 - (1.8 \cdot 10^7)t + (1.8 \cdot 10^{10}) \quad (48)$$

Individual expressions for the conditional probability of an attack must be addressed for the conditional expression in (24). This study created probabilistic distribution models in (47) and (48) for the conditional expression based on the Bayesian approach to statistics; adopting Bayes' Theorem:

$$P^* = P_{n,s}(\lambda | \theta) \quad (49)$$

$$= \frac{P(\lambda) \cdot L(\theta_{n,s}, \dots, \theta_{n,7} | \lambda_{s,i})}{P(\theta)} \quad (50)$$

$$\propto P(\lambda) \cdot L(\theta_{n,s} | \lambda_{s,i}) \quad (51)$$

where, L , represents the likelihood function associated with the aggregation of information assurance service threats, and assuming common threats are defined dynamically over time, such that:

$$\lim_{t \rightarrow \infty} P_{n,s}[\theta(t)] = 1 \quad (52)$$

The adoption of Bayes' rule to PRA shows that if given (52), or given that a threat event θ exists, then the relevant sample space is reduced to θ , because θ is true; the conditional probability in (49) becomes a probability measure on θ as expressed in (51).

Data

The DoDI 8500.2 DIACAP control checklists for MAC I, II, and III classified systems, have all been consolidated to create a single checklist, shown below as Table 3. DIACAP IA control checklists are helpful in analyzing controls in an efficient and systematic manner (NIST SP 800-30, 2002). For the purposes of this study, and from the scope defined in (19), this paper adopts Table 3 as a conventional inventory for CIS vulnerabilities and controls.

Table 3

DoDI 8500.2 Controls for Classified Systems

DIACAP VULNERABILITIES / CONTROLS FOR CLASSIFIED SYSTEMS (MAC I, II, III)				
INDEX	CONTROL	VUL DESCRIPTION	IMPACT	ISS
s,i	$\delta_{s,i}$	$D_{s,i}$	$\omega_{s,i}$	S,n
Physical Security IAS (s = 1)				
1,1	PEPF-2	Physical Protection of Facilities 2	1	CONF
1,2	PESS-1	Storage	1	CONF
1,3	PEVC-1	Visitor Control to Computing Facilities	1	CONF
1,4	PECF-2	Access to Computing Facilities 2	1	CONF
1,5	PECS-2	Clearing and Sanitizing 2	1	CONF
1,6	PEDD-1	Destruction	1	CONF
1,7	PEDI-1	Data Interception	1	CONF
1,8	PEFD-2	Fire Detection 2	1	AVAIL
1,9	PEFS-2	Fire Suppression System 2	1	AVAIL
1,10	PEMS-1	Master Power Switch	1	AVAIL
1,11	PEFD-1	Fire Detection	1	AVAIL
1,12	PEVR-1	Voltage Regulators	1	AVAIL
1,13	PESP-1	Workplace Security Practices	2	CONF
1,14	PEFS-1	Fire Suppression System	2	AVAIL
1,15	PEHC-1	Humidity Controls	2	AVAIL
1,16	PEEL-2	Emergency Lighting 2	2	AVAIL
1,17	PEFI-1	Fire Inspection	2	AVAIL
1,18	PEHC-2	Humidity Controls 2	2	AVAIL
1,19	PETC-2	Temperature Controls 2	2	AVAIL
1,20	PEPS-1	Physical Security Testing	3	CONF
1,21	PEEL-1	Emergency Lighting	3	AVAIL
1,22	PETC-1	Temperature Controls	3	AVAIL
1,23	PETN-1	Environmental Control Training	3	AVAIL
Cyber Security IAS (s = 2)				
2,1	EBRP-1	Remote Access for Privileged Functions	1	CONF
2,2	EBRU-1	Controlled Remote Access	1	CONF
2,3	ECCR-3	Encryption of Data at Rest (SAMI)	1	CONF
2,4	ECCT-2	Encryption for Data in Transit 2	1	CONF
2,5	ECIC-1	Interconnection Control Interfaces	1	CONF
2,6	ECTC-1	Tempest Requirements	1	CONF
2,7	DCSR-3	Robustness Protection Profile - High	1	CONF
2,8	DCSS-1	System State Changes	1	INT
2,9	ECTM-2	Transmission Integrity Controls 2	1	INT
2,10	DCSW-1	Baseline Software Inventory	1	AVAIL
2,11	ECVP-1	Anti-Virus Software	1	AVAIL
2,12	ECWN-1	Wireless Computing and Networking	1	AVAIL
2,13	ECCR-1	Encryption of Data at Rest (Non-SAMI)	2	CONF
2,14	ECCR-2	Encryption for Data at Rest 2	2	CONF

2,15	ECNK-1	Encrypting Need-To-Know in Transit	2	CONF
2,16	ECNK-2	Encrypting Need-To-Know in Transit (SAMI) 2	2	CONF
2,17	ECRC-1	Object Reuse	2	CONF
2,18	PESL-1	Screen Lock	2	INT
2,19	ECTM-1	Transmission Integrity Controls	2	INT
2,20	ECID-1	Host Based IDS	2	INT
2,21	ECIM-1	Instant Messaging	2	INT
2,22	ECND-2	Network Device Control Program 2	2	INT
2,23	DCSP-1	Security Support Structure Partitioning	2	INT
2,24	DCSQ-1	Software Quality Requirements	2	INT
2,25	DCSS-2	Secure State Assurance 2	2	INT
2,26	DCSL-1	System Library Management Controls	2	INT
2,27	DCMC-1	Mobile Code	2	INT
2,28	DCNR-1	Non-Repudiation	2	INT
2,29	DCPD-1	Public Domain Software Controls	2	AVAIL
2,30	DCPP-1	Ports, Protocols, and Services	2	AVAIL
2,31	EBVC-1	IDS VPN Traffic Visibility	2	AVAIL
2,32	ECVI-1	VOIP	2	AVAIL
2,33	EBBD-3	Boundary Defense	3	CONF
2,34	DCPA-1	Partitioning the Application	3	INT
2,35	ECND-1	Network Device Controls	3	INT
Continuity IAS (s = 3)				
3,1	COAS-2	Alternate Site Designation	1	AVAIL
3,2	COBR-1	Backup and Restoration Asset Protection	1	AVAIL
3,3	COEB-2	Alternate Site Enclave Boundary Defense	1	AVAIL
3,4	COSW-1	Backup Copies of Critical Software	1	AVAIL
3,5	CODB-3	Data Backup Procedures	2	AVAIL
3,6	CODP-3	Disaster and Recovery Plan	2	AVAIL
3,7	COMS-2	Maintenance Support	2	AVAIL
3,8	COPS-3	Power Supply	2	AVAIL
3,9	COSP-2	Spares and Parts	2	AVAIL
3,10	COAS-1	Alternate Site Designation	2	AVAIL
3,11	COSP-1	Spares and Parts	2	AVAIL
3,12	CODP-2	Disaster and Recovery Planning 2	2	AVAIL
3,13	COEB-1	Enclave Boundary Defense	2	AVAIL
3,14	COMS-1	Maintenance Support	2	AVAIL
3,15	COPS-2	Power Supply 2	2	AVAIL
3,16	COPS-1	Power Supply	3	AVAIL
3,17	CODP-1	Disaster and Recovery Planning	3	AVAIL
Security Design, Configuration, Operations & Administration IAS (s = 4)				
4,1	DCAS-1	Acquisition Standards	1	CONF
4,2	ECCM-1	COMSEC (C-5200.5)	1	CONF
4,3	ECMT-2	Conformance Monitoring and Testing	1	CONF
4,4	DCCS-2	Configuration Specifications	1	INT
4,5	DCID-1	Interconnection Documentation	1	INT
4,6	DCIT-1	IA for IT Services	1	INT

4,7	DCPR-1	CM Process	1	INT
4,8	ECAR-3	Audit Record Content	1	INT
4,9	DCCS-1	Configuration Specifications	1	INT
4,10	ECSD-2	Software Change Controls	1	INT
4,11	COTR-1	Trusted Recovery	1	AVAIL
4,12	DCHW-1	HW Baseline	1	AVAIL
4,13	DCPB-1	IA Program and Budget	1	AVAIL
4,14	ECSC-1	DoD Security Configuration Guide	1	AVAIL
4,15	VIIR-2	Incident Response Planning 2	1	AVAIL
4,16	VIVM-1	Vulnerability Management	1	AVAIL
4,17	DCBP-1	Best Security Practices	2	INT
4,18	DCCB-2	Control Board	2	INT
4,19	DCII-1	IA Impact Assessment	2	INT
4,20	ECDC-1	Transaction Journaling	2	INT
4,21	ECAT-2	Audit Record Review	2	INT
4,22	DCDS-1	Dedicated IA Services	2	INT
4,23	DCFA-1	Functional Architecture for AIS Apps	2	INT
4,24	ECRR-1	Audit Record Retention	2	INT
4,25	ECTB-1	Audit Record Backup	2	INT
4,26	ECTP-1	Audit Record Protection	2	INT
4,27	ECSD-1	Software Change Controls	2	INT
4,28	COEF-2	Identification of Essential Functions	2	AVAIL
4,29	DCAR-1	Procedural Review	2	AVAIL
4,30	EBCR-1	Connection Rules	2	AVAIL
4,31	DCCT-1	Compliance Testing	2	AVAIL
4,32	CODB-2	Data Backup Procedures 2	2	AVAIL
4,33	VIIR-1	Incident Response Planning	2	AVAIL
4,34	ECLC-1	Audit of Security Labels	3	CONF
4,35	DCCB-1	Control Board	3	INT
4,36	ECRG-1	Audit Tools	3	INT
4,37	ECAT-1	Audit Trail, Monitoring, Reporting	3	INT
4,38	CODB-1	Data Backup Procedures	3	AVAIL
4,39	COEF-1	Identification of Essential Functions	3	AVAIL
Security Education, Training and Awareness IAS (s = 5)				
5,1	ECWM-1	Warning Message	1	CONF
5,2	PRTN-1	Information Assurance Training	1	INT
5,3	DCSD-1	IA Documentation	1	AVAIL
5,4	PRRB-1	Security Rules of Behavior	1	AVAIL
5,5	COED-2	Scheduled Exercises of COOP/DRP	2	AVAIL
5,6	COED-1	Scheduled Exercises and Drills	3	AVAIL
Identity Authentication and Authorization IAS (s = 6)				
6,1	IAIA-2	Indv. Identification and Authentication	1	CONF
6,2	IAAC-1	Comprehensive Account Management Process	1	CONF
6,3	ECLP-1	Separation of Duties & Least Privilege	1	CONF
6,4	IAIA-1	Indv. Identification and Authentication	1	CONF
6,5	PRAS-2	Access to Information	1	CONF

6,6	PRMP-2	Maintenance Personnel 2	1	CONF
6,7	PRNK-1	Access to Need-to-Know Information	1	CONF
6,8	ECPA-1	Role-Based Access	1	INT
6,9	IAGA-1	Group Authenticator Usage	2	CONF
6,10	ECAD-1	Affiliation Identification	2	CONF
6,11	ECLO-2	Logon Attempts & Limited Sessions	2	CONF
6,12	ECPC-2	Application Programmer Privilege Control	2	INT
6,13	IAKM-3	Key Management	2	INT
6,14	IATS-2	Token and Certification Standards	2	INT
6,15	ECPC-1	Production Code Change Controls	2	INT
6,16	IAKM-1	Key Management	2	INT
6,17	IAKM-2	Key Management 2	2	INT
6,18	IATS-1	Token and Certification Standards	2	INT
Information Content Security IAS (s = 7)				
7,1	ECAN-1	Access to Data	1	CONF
7,2	ECML-1	Marking and Labeling	1	CONF
7,3	ECCD-2	Access Control Mechanisms	1	INT
7,4	ECCD-1	Changes to Data	2	INT

The qualitative value derived for a CIS is based on IA constraints. The following DIACAP IA test constraints, each identified by a condition identification (ID) letter, within Table 4 below, for MAC I, II, and III CIS, is utilized as a component for the analysis of proposed family of quantitative risk expressions, consisting of (40), (43), and (46). The component of IA categorization will allow this study to develop a population sample of CIS test models.

Table 4

Possible IA Constraints for CIS

ID	CONSTRAINT DESCRIPTION
A	SYSTEM CONTAINS A NON-COMPLIANT IMPACT CAT 1 FINDING (FAIL)
B	SYSTEM CONTAINS A NON-COMPLIANT IMPACT CAT 2 FINDING
C	SYSTEM CONTAINS A NON-COMPLIANT IMPACT CAT 3 FINDING
I	NON-COMPLIANT CONTROL / VUL AFFECTING ISS: CONFIDENTIALITY
J	NON-COMPLIANT CONTROL / VUL AFFECTING ISS: INTEGRITY
K	NON-COMPLIANT CONTROL / VUL AFFECTING ISS: AVAILABILITY
Q	NON-COMPLIANT CONTROL / VUL AFFECTING IAS (s = 1): PHYSICAL SECURITY

R	NON-COMPLIANT CONTROL / VUL AFFECTING IAS (s = 2): CYBER SECURITY
S	NON-COMPLIANT CONTROL / VUL AFFECTING IAS (s = 3): CONTINUITY SECURITY
T	NON-COMPLIANT CONTROL / VUL AFFECTING IAS (s = 4): SECURITY DESIGN
U	NON-COMPLIANT CONTROL / VUL AFFECTING IAS (s = 5): SECURITY TRAINING
V	NON-COMPLIANT CONTROL / VUL AFFECTING IAS (s = 6): IDENTITY A&A
W	NON-COMPLIANT CONTROL / VUL AFFECTING IAS (s = 7): INFORMATION CONTENT
Y	FULLY COMPLIANT SYSTEM (ALL CONTROLS / VULS COMPLIANT)
P	SYSTEM CONTAINS AT LEAST A SINGLE CONFIDENCE ADJUSTMENT
X	SYSTEM CONTAINS AN INDIVIDUAL QUALITATIVE IAS SCORE BELOW <60% (FAIL)
Z	FULLY NON-COMPLIANT SYSTEM (ALL CONTROLS / VULS NON-COMPLIANT)

The total population, or possible distinguishable combination of constrained CIS models,

C_{TOTAL} , created for this study is expressed by the following binomial combination:

$$C_{TOTAL} = 2 \times \sum_{n\{P\}} \left[\sum_{r=1}^3 \binom{3}{r} \right] \cdot \left[\sum_{r=1}^3 \binom{3}{r} \right] \cdot \left[\sum_{r=1}^7 \binom{7}{r} - 23 \right] + 1_{n\{Y\}} \tag{53}$$

$$C_{TOTAL} = 2 \times [{}_3C_3 + {}_3C_2 + {}_3C_1] \cdot [{}_3C_3 + {}_3C_2 + {}_3C_1] \cdot [{}_7C_7 + {}_7C_6 + {}_7C_5 + {}_7C_4 + {}_7C_3 + \dots \\ \dots + {}_7C_2 + {}_7C_1 - 23] + 1 \tag{54}$$

$$C_{TOTAL} = 11,939 \tag{55}$$

The population of possible IA constraints, within Table 4, allows for the development of a consolidated sample of qualitative DIACAP scorecard results, for CIS models representing validation and acceptance criteria, with compliant and non-compliant controls strategically selected in being able to analyze significant thresholds. The data sample of CIS models, each identified by a unique constraint combination ID, is listed with its associated qualitative DIACAP IA percentage score in Table 5.

The sample size amount, s , of test models, to statistically represent the total possible qualitative IA risk assessment constraints combinations of those models, is commonly expressed by

$$s = \frac{s_0}{\left(1 + \frac{s_0 - 1}{C_{\text{TOTAL}}}\right)} \quad (56)$$

and, for this study, calculated to be

$$s \approx 100 \quad (57)$$

, where

$$s_0 = \frac{Z^2 p(1-p)}{e^2} \quad (58)$$

, with the probability (confidence) of the sample, falling within (or representing) 84.1% of the population distribution, (Z-value) as

$$Z = +1\sigma \quad (59)$$

, assuming a maximum degree of variability (less homogenous of a population),

$$p = 0.50 \quad (60)$$

, in the constraints outlined, is also dependent on the desired level of precision ($\pm 5\%$ confidence interval) where

$$e = 0.05 \quad (61)$$

Table 5

CIS Test Models and Qualitative DIACAP IA Scorecard Data Sample

MODEL/CONSTRAINT ID	INFORMATION ASSURANCE SERVICE (IAS), s =							TOTAL
	1	2	3	4	5	6	7	
CIS01/Y	100%	100%	100%	100%	100%	100%	100%	100%
CIS02/CQRSTUVWIJKP	100%	100%	100%	100%	100%	100%	100%	100%
CIS03/CQRSTUVWIP	100%	100%	100%	100%	100%	100%	100%	100%
CIS04/CQRSTUVWJP	100%	100%	100%	100%	100%	100%	100%	100%
CIS05/CQRSTUVWKP	100%	100%	100%	100%	100%	100%	100%	100%
CIS06/BQRSTUVWIJKP	100%	100%	100%	100%	100%	100%	100%	100%
CIS07/BQRSTUVWIP	100%	100%	100%	100%	100%	100%	100%	100%
CIS08/BQRSTUVWJP	100%	100%	100%	100%	100%	100%	100%	100%
CIS09/BQRSTUVWKP	100%	100%	100%	100%	100%	100%	100%	100%
CIS10/CQI	95%	100%	100%	100%	100%	100%	100%	95%
CIS11/CQK	95%	100%	100%	100%	100%	100%	100%	95%
CIS12/CRI	100%	95%	100%	100%	100%	100%	100%	95%
CIS13/CRJ	100%	95%	100%	100%	100%	100%	100%	95%
CIS14/CSK	100%	100%	95%	100%	100%	100%	100%	95%
CIS15/CTI	100%	100%	100%	95%	100%	100%	100%	95%
CIS16/CTJ	100%	100%	100%	95%	100%	100%	100%	95%
CIS17/CTK	100%	100%	100%	95%	100%	100%	100%	95%
CIS18/CUK	100%	100%	100%	100%	95%	100%	100%	95%
CIS19/CQRIJ	95%	95%	100%	100%	100%	100%	100%	95%
CIS20/CQRSIJK	95%	95%	95%	100%	100%	100%	100%	95%
CIS21/CQRSTIJK	95%	95%	95%	95%	100%	100%	100%	95%
CIS22/CQRSTUIJK	95%	95%	95%	95%	95%	100%	100%	95%
CIS23/BQI	90%	100%	100%	100%	100%	100%	100%	90%
CIS24/BQK	90%	100%	100%	100%	100%	100%	100%	90%
CIS25/BRI	100%	90%	100%	100%	100%	100%	100%	90%
CIS26/BRJ	100%	90%	100%	100%	100%	100%	100%	90%
CIS27/BRK	100%	90%	100%	100%	100%	100%	100%	90%
CIS28/BSK	100%	100%	90%	100%	100%	100%	100%	90%
CIS29/BTJ	100%	100%	100%	90%	100%	100%	100%	90%
CIS30/BTK	100%	100%	100%	90%	100%	100%	100%	90%
CIS31/BUK	100%	100%	100%	100%	90%	100%	100%	90%
CIS32/BVI	100%	100%	100%	100%	100%	90%	100%	90%
CIS33/BVK	100%	100%	100%	100%	100%	90%	100%	90%
CIS34/BWJ	100%	100%	100%	100%	100%	100%	90%	90%
CIS35/BQRIJK	90%	90%	100%	100%	100%	100%	100%	90%
CIS36/BQRSIJK	90%	90%	90%	100%	100%	100%	100%	90%

CIS37/BQRSTIJK	90%	90%	90%	90%	100%	100%	100%	90%
CIS38/BQRSTUIJK	90%	90%	90%	90%	90%	100%	100%	90%
CIS39/BQRSTUVIJK	90%	90%	90%	90%	90%	90%	100%	90%
CIS40/BQRSTUVWIJK	90%	90%	90%	90%	90%	90%	90%	90%
CIS41/AQI	60%	100%	100%	100%	100%	100%	100%	60%
CIS42/AQK	60%	100%	100%	100%	100%	100%	100%	60%
CIS43/ARI	100%	60%	100%	100%	100%	100%	100%	60%
CIS44/ARJ	100%	60%	100%	100%	100%	100%	100%	60%
CIS45/ARK	100%	60%	100%	100%	100%	100%	100%	60%
CIS46/ASK	100%	100%	60%	100%	100%	100%	100%	60%
CIS47/ATI	100%	100%	100%	60%	100%	100%	100%	60%
CIS48/ATJ	100%	100%	100%	60%	100%	100%	100%	60%
CIS49/ATK	100%	100%	100%	60%	100%	100%	100%	60%
CIS50/AUI	100%	100%	100%	100%	60%	100%	100%	60%
CIS51/AUJ	100%	100%	100%	100%	60%	100%	100%	60%
CIS52/AUK	100%	100%	100%	100%	60%	100%	100%	60%
CIS53/AVI	100%	100%	100%	100%	100%	60%	100%	60%
CIS54/AVJ	100%	100%	100%	100%	100%	60%	100%	60%
CIS55/AVI	100%	100%	100%	100%	100%	70%	60%	60%
CIS56/AVJ	100%	100%	100%	100%	100%	70%	60%	60%
CIS57/AQRIK	60%	60%	100%	100%	100%	100%	100%	60%
CIS58/AQRSIJK	60%	60%	60%	100%	100%	100%	100%	60%
CIS59/AQRSTIJK	60%	60%	60%	60%	100%	100%	100%	60%
CIS60/AQRSTUIJK	60%	60%	60%	60%	60%	100%	100%	60%
CIS61/AQRSTUVIJK	60%	60%	60%	60%	60%	60%	100%	60%
CIS62/AQRSTUVWIJK	60%	60%	60%	60%	60%	60%	60%	60%
CIS63/BCQRSTUI	90%	95%	95%	95%	95%	100%	100%	90%
CIS64/BCQRSTUK	90%	95%	95%	95%	95%	100%	100%	90%
CIS65/BCQRSTUI	95%	90%	95%	95%	95%	100%	100%	90%
CIS66/BCQRSTUJ	95%	90%	95%	95%	95%	100%	100%	90%
CIS67/BCQRSTUK	95%	90%	95%	95%	95%	100%	100%	90%
CIS68/BCQRSTUK	95%	95%	90%	95%	95%	100%	100%	90%
CIS69/BCQRSTUJ	95%	95%	95%	90%	95%	100%	100%	90%
CIS70/BCQRSTUK	95%	95%	95%	90%	95%	100%	100%	90%
CIS71/BCQRSTUK	95%	95%	95%	95%	90%	100%	100%	90%
CIS72/BCQRSTUI	95%	95%	95%	95%	95%	90%	100%	90%
CIS73/BCQRSTUK	95%	95%	95%	95%	95%	90%	100%	90%
CIS74/BCQRSTUJ	95%	95%	95%	95%	95%	100%	90%	90%
CIS75/ABQRSTUVWI	60%	90%	90%	90%	90%	90%	90%	60%
CIS76/ABQRSTUVWK	60%	90%	90%	90%	90%	90%	90%	60%
CIS77/ABQRSTUVWI	90%	60%	90%	90%	90%	90%	90%	60%
CIS78/ABQRSTUVWJ	90%	60%	90%	90%	90%	90%	90%	60%

CIS79/ABQRSTUWVK	90%	60%	90%	90%	90%	90%	90%	60%
CIS80/ABQRSTUWVK	90%	90%	60%	90%	90%	90%	90%	60%
CIS81/ABQRSTUWVI	90%	90%	90%	60%	90%	90%	90%	60%
CIS82/ABQRSTUWVJ	90%	90%	90%	60%	90%	90%	90%	60%
CIS83/ABQRSTUWVK	90%	90%	90%	60%	90%	90%	90%	60%
CIS84/ABQRSTUWVI	90%	90%	90%	90%	60%	90%	90%	60%
CIS85/ABQRSTUWVJ	90%	90%	90%	90%	60%	90%	90%	60%
CIS86/ABQRSTUWVK	90%	90%	90%	90%	60%	90%	90%	60%
CIS87/ABQRSTUWVI	90%	90%	90%	90%	90%	60%	90%	60%
CIS88/ABQRSTUWVJ	90%	90%	90%	90%	90%	60%	90%	60%
CIS89/ABQRSTUWVI	90%	90%	90%	90%	90%	90%	60%	60%
CIS90/ABQRSTUWVJ	90%	90%	90%	90%	90%	90%	60%	60%
CIS91/BCQRSTUWVIJKP	60%	60%	60%	60%	60%	60%	60%	60%
CIS92/BCQRSTUWVIJKXP	50%	50%	50%	50%	50%	50%	50%	50%
CIS93/CQRSTUWVIJK	85%	85%	90%	70%	95%	100%	100%	70%
CIS94/CQRSTUWVI	85%	80%	100%	70%	100%	100%	100%	70%
CIS95/CQRSTUWVJ	100%	80%	100%	70%	100%	100%	100%	70%
CIS96/CQRSTUWVK	85%	70%	90%	70%	95%	100%	100%	70%
CIS97/BQRSTUWVIJKX	30%	-100%	-10%	-70%	90%	0%	90%	0%
CIS98/BQRSTUWVIX	90%	50%	100%	100%	100%	70%	100%	50%
CIS99/BQRSTUWVJX	100%	-10%	100%	-10%	100%	30%	90%	0%
CIS100/BQRSTUWVKX	40%	60%	-10%	40%	90%	100%	100%	0%
CIS101/AQRSTUWVIJKX	-380%	-380%	-60%	-540%	-60%	-220%	-20%	0%
CIS102/AQRSTUWVI	-280%	-280%	100%	-20%	60%	-180%	20%	0%
CIS103/AQRSTUWVJX	100%	20%	100%	-180%	60%	60%	60%	0%
CIS104/AQRSTUWVKX	-100%	-20%	-60%	-140%	20%	100%	100%	0%
CIS105/BCQRSTUWVIJKXP	0%	0%	0%	0%	0%	0%	0%	0%
CIS106/Z	-470%	-595%	-180%	-740%	-75%	-320%	-30%	0%

Procedure

Thus far, this chapter has been able to address both research questions (Q1 and Q2), in showing that a continuous, time-dependent, quantitative risk expression and corresponding risk determination metric for CIS are, in fact, possible to create, given existing Probabilistic Risk Assessment (PRA) techniques. However, how does the reader know for sure if these expressions are truly meaningful or not? Answer: Validation by parts - viability and integrity

testing of the quantitative models. This section explains the validation procedures taken to properly test and analyze the derived quantitative expressions for the SRA of CIS.

By ‘viability testing’, this paper means to apply the family of derived risk expressions, toward the given IA constraints within Table 4; comparing against a sample of resulting quantitative data values from CIS test models listed in Table 5, ultimately, to feasibly conduct risk determinations that can be compared and validated with existing qualitative results.

By ‘integrity testing’, this study means to conduct analysis on all individual risk elements that include both small and large damage potentials. Sensitivity analysis will show to what extent the viability of the quantitative risk expressions is influenced by variations in quantifiable variables. Many sources of technological risks have a very high disaster potential, although, the probability that this potential manifests as damage is extremely low. Thus, the prime characteristics, within this risk class, that will be of interest, within the analysis of the following chapter, are its combination of low probability with a high extent of damage (Klinke, 2006). This procedure for investigating the impact of changes in variables on the base-case (most probable outcome scenario) ultimately provides support for a meaningful interpretation of the expressions (Q1 & Q2, WBS 1.1 & 1.2).

In examining the unique quantitative risk determination metric for SRA-CIS, sensitivity analysis (WBS 1.2.6), is conducted in the following chapter, allowing for the calibration, and actual measurement, of meaningful risk acceptance thresholds (WBS 1.2.3), as listed in Table 2. Upon final validation, multivariate analysis is applied to (i) create further meaningful risk relationships, (ii) specifically to include the ISS CIA competing constraints triad, and between (iii) individual quantitative and qualitative risk elements.

Assumptions

A number of assumptions are made within this case study, one of which involves the confidence factor interpreted in (23) for the quantitative, time-dependent risk expression in (43). Notice that the confidence factor is time-dependent itself. A CIS containing a non-compliant control finding, with its mitigation action addressed within a POA&M, to be completed within an allocated Δt , should have its risk-confidence adjustment after the, Δt , period has elapsed. However, the introduction of time-dependence and various Δt values for the confidence variable greatly increases the number of possible IA constraint combinations for analysis, creating unnecessary complexity. Thus, for confidence adjustments, the assumption made is that $\Delta t = 0$.

Another assumption that requires attention is based on the fact that a DAA can adjust the qualitative severity categories for IA controls based on system characteristics and the nature of the data. Although this condition can be adequately addressed by making corresponding adjustments to the confidence parameter, dynamic manipulation of severity category adjustments would also contribute to an increased number of possible IA constraint combinations for analysis, resulting in unwanted complexity. This study is focused only on MAC I, CIS and makes the assumption that such adjustments are not made.

False assumptions are commonly made between quantitative and qualitative risk analysis, one of which associates quantitative risk analysis with objectivity, and qualitative methods with subjectivity, due to the use and non-use of numerical methods. It is extremely important to highlight this false dichotomy, and that quantitative risk analysis (QRA) results should not be the sole basis for decision making by responsible authorities. The purpose of

this study is to explore and highlight the viability of QRA for CIS; not to dismiss qualitative methods for quantitative ones.

Research Questions

Research Question 1 (RQ1).

Is it possible to create a meaningful continuous, time-dependent, quantitative risk expression for CIS given existing security risk analysis (SRA) techniques?

Test Method: An exploratory approach, in proposing a continuous, time-dependent, quantitative CIS risk expression, is taken in arriving at (43). Multivariate analysis (MVA) is used in being able to observe and analyze more than one risk element at a time; with established models and data in Tables 4 & 5, analysis will reveal the meaningful constraints, and relationships of risk elements previously identified, and ultimately, support the proposed general risk expression itself. As the name indicates, MVA comprises a set of techniques dedicated to the analysis of data sets with more than one variable (Abdi, 2003). This paper analyzes two sets of data: the first data set belonging to risk predictors, or independent variables (IV), and the second set corresponding to the qualitative and quantitative risk measurements, or dependent variables (DV).

Research Question 2 (RQ2).

Is it possible to create a meaningful continuous, time-dependent, quantitative risk determination metric for CIS from a risk expression?

Test Method: The creation of a continuous, time-dependent, quantitative risk determination metric, as in (46), is first contingent on being able to satisfy the previous

research question, and the creation of a continuous, time-dependent, quantitative CIS risk expression (43). MVA discussed for RQ1 is similarly adopted for use in RQ2, using principal component analysis (PCA), and one data set. With a PCA approach, the decomposition of the correlated risk result measurements from RQ1 are brought into a new set of uncorrelated variables, or principal components, whose measurements are projected on (46) to support the validity of the risk determination metric.

Strengths and Weaknesses

Strengths

The methodology presented for this empirical study provides strong support for the quantitative proposal of risk, comparative analysis, and resulting meaningful inferences using a data sample from the qualitative population, and corresponding time-dependent quantitative results. In designing the sample test models, within Table 5, that significantly represents the constraint population in Table 4, (59), (60), and (61) were conservatively chosen to create sufficient statistical power.

Weaknesses

To truly determine whether a time-dependent risk expression is accurate to qualitative risk assessments, one would outline a method to test a number of model systems by arriving at risk and determination values for some future time t , and then follow up after time t , to conduct a comparative analysis between existing qualitative values. However, such a method is not within the scope of this case study and does not meet the primary research objective of this paper, namely, the meaningful interpretation, versus accuracy, of a time-dependent family

of risk expressions.

As discussed and expressed in (49), the application of the Bayesian approach is adopted in dealing with the evaluation of (24), however, its inherent weakness lies with the assessment of the likelihood function, as it must capture the interrelationships among γ and $\theta_{n,s}, \dots, \theta_{n,7}$, accounting for precision and bias, in modeling dependence among threats (Clemen, 1997). Additionally, remember the expression introduced earlier about ‘getting out what you put in?’ The statistics or lack thereof, to accurately represent a commutative time-dependent risk for CIS, as in (43), remains the primary weakness in the application of the outlined methodology. There are no publicly accessible databases, tracking current CIS threats, acting on generalized categories of vulnerabilities, let alone, specific vulnerabilities as listed in DIACAP.

Chapter Summary

A number of methodologies are outlined within this chapter, adopting the use of probabilistic measures to begin getting a handle on risk, defining a formal time-dependent risk expression, and logically extending these measures into a risk determination metric for CIS. The next chapter uses simple sensitivity analysis on our risk relationships, to consider how varied changes to unique risk elements influences overall risk, and testing thresholds examined through case studies with unique IA constraints from CIS currently in operation. This exercise attempts to meet two major objectives: first, to enhance the reader’s competence in the actual application of the derived risk expressions and, second, to increase confidence in the risk relationships formulated from this analysis. Lastly, the concluding chapter summarizes the major findings of this paper and draws some more general conclusions.

CHAPTER 4

ANALYSIS

Purpose of the Chapter

As previously introduced, Security Risk Analysis is essentially segmented into two types of approaches: *quantitative* and *qualitative*. The purpose of this chapter, and ultimately of this paper, is to interpret, assess, and validate the meaningfulness of a quantitative approach to SRA, as proposed, for CIS (RQ1). Furthermore, the results, meaningful patterns, and metrics identified from this analysis serves to define the boundaries of a quantitative risk determination framework (RQ2).

This chapter provides an analysis of the security risks associated with CIS using techniques and reasoning that examine prime characteristics, investigating the impact of changes in variables on the base case, to validate meaningful relationships; enhancing competence in the actual application of the derived risk expressions and increased confidence in the risk relationships formulated by this paper.

The extent of the required analysis and deliberation for SRA-CIS is contingent upon circumstances surrounding the risk under consideration (Klinke, 2002). In line with this reasoning, this thesis began by providing its reader with a background in risk and security risk analysis, specifically, addressing the overarching issues behind both purely qualitative and quantitative SRA methods. The identified issues yielded guiding elements for the presentation of an analytic approach toward risk evaluation and rational risk decision making.

Chapter Organization

Moving forward, from this point in the chapter, are four organized main sections. The first section, a preliminary analysis subdivided into two parts, includes (i) a descriptive examination of the ISS (CIA), as the primary adopted unit of measurement (risk dimension), for quantified risks associated with CIS, and (ii) a preliminary analysis of probabilistic estimates based on the probabilistic distribution models, quantitative approach, and methodologies presented by this paper.

Second, the reliability of the data used and the subsequent analysis conducted, within this paper, are detailed. As the subject of uncertainty, generally associated with risk has been discussed, the uncertainties quantified using probabilistic estimations, is of particular interest, and further discussed in terms of data reliability (strength of evidence).

For the third section, titled SRA, also subdivided by both research questions RQ1 and RQ2, (i) a study of the viability and meaningful interpretation between both quantitative and qualitative SRA approaches is conducted, where the family of derived risk expressions is applied toward corresponding models, sampled from IA constraints defined for CIS, through formal procedures and analysis methods outlined within the previous chapter; (ii) a new set of principal elements, decomposed from resulting risk measurement values of RQ1 CIS test models, are projected onto (46), and examined in conducting risk determinations required for the analysis and validity of a risk determination framework. Analysis of the determination metric in (46), specifically for each individual ISS risk dimension element (CIA), is compared to CIS MAC levels, as defined by DoDI 8500.2, and as listed within Table 2, to arrive at appropriate risk boundary values and formally present a risk acceptance framework for risk decisions.

Finally, in the fourth section, the chapter concludes by highlighting new relationships established from the analysis of RQ1 and RQ2. This is, primarily, an interpretation of the results from this analysis.

Preliminary Analysis

Throughout this chapter, sensitivity analysis was employed to evaluate how varied changes to unique risk elements influences overall risk; testing thresholds examined through case studies with unique IA constraints. Additionally, consideration on the effect of risk elements/predictors (input variables) on qualitative and quantitative risk measurements (dependent variables) is made, of the proposed approach, to include logical relationships among assertions, observations, and the analysis of more than one risk element at a time, revealing meaningful constraints and relationships between the risk elements themselves, as it supports the proposed general risk expression.

Descriptive Statistics

As was touched upon in Chapter 3, Quantitative SRA requires one to reanalyze the unit of measure for risk. To this effect, the discussion of a comprehensive and meaningful expression of risk is extended, for CIS, with an adopted risk measurement, namely, in terms of the *confidence*, in which one has, for the loss of each of the Information Security Services (ISS) or risk dimensions: Confidentiality, Integrity, and Availability (CIA). This differs from the interpretation of a risk metric that is based solely on cost. As indicated, the expected value of risk is bounded by unity $(0,1]$, where risk is never zero. The unit risk measurement, adopted for each ISS dimension, IAS, or more generally, each risk element, while also bounded by unity, takes on a different interpretation, when expressed in terms of confidence versus risk.

Recall from (7), that risk is a function of uncertainty, and from (6), that uncertainty refers to the degree to which one lacks confidence, thus,

$$\text{Risk}_{EV} = 100\% - (\text{Risk Loss Confidence}) \quad (62)$$

or

$$R_{LC} = 1 - R_{EV} \quad (63)$$

where

$$0\% \leq \text{Risk Loss Confidence} < 100\% \quad (64)$$

The meaningful interpretation of this unit of measurement reads, for example, as: ‘0.85A’, or the risk as having ‘85% confidence in the loss of availability of the CIS’. This, based on the EV-LC relationship in (63), corresponds to an expected value of risk, R_{EV} , equal to 0.15. Note that the upper bound of the Risk Loss Confidence inequality in (64), is open, and never equal to 100%. This may come as a surprise to the reader, however as given in (30), that the expected value of risk is never zero, and thus from (63), one should, in fact, not expect a 100% Risk Confidence (or 100% confidence in the loss) of any ISS:

$$R_{LC} \neq 1 \quad (65)$$

A risk dimension is able to factor interchangeably with another following the generalized ISS triad property, as illustrated in Figure 3, a general relationship that is expressed in (20), further defined and governed by the cumulative product of N risks in (28). The risk measurement, for the total information security risk appraisal, is able to maintain the boundary of unity through averaging, by the number of ISS or risk dimensions, N :

$$\text{Total Information Security Risk Appraisal} = \frac{1}{N} \sum_{n=1}^N (\text{ISS})_n \quad (66)$$

More specifically, for ISS (CIA), the security risk appraisal, or R_{TOTAL} , then becomes

$$R_{TOTAL} = \frac{1}{3}(\text{CONF}_{n=1} + \text{INT}_{n=2} + \text{AVAIL}_{n=3}) \quad (67)$$

In contrast, the total percentage scores seen from Table 5, Qualitative DIACAP IA Scorecard Data Sample Table, reflects an overall Information Security Domain (ISD) appraisal score of:

$$\text{Security Confidence} = \min(|\text{IAS}|_{s=1}, \dots, |\text{IAS}|_{s=7}) \quad (68)$$

The following figure below illustrates the relationship between the expected value of risk, R_{EV} , and risk loss confidence, R_{LC} , as a function of an increased cumulative product of risks.

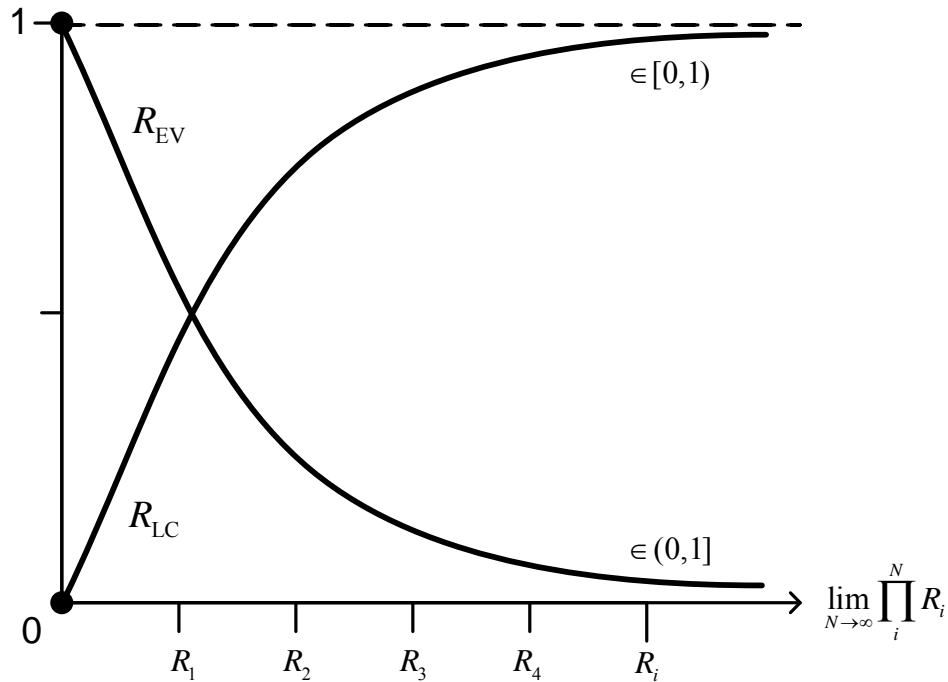


Figure 7. Expected Value and Risk Loss Confidence versus Cumulative Risk Product

As risk denotes an uncertain outcome, the issue of uncertainty itself, has become a major topic of debate within the risk community. Approaching an analysis of uncertainty, as it pertains to risk, begins with the identification of probabilities linked to specific adverse effects. The term “probability of occurrence” is adopted for risk events in which information and data on past trends or cyclical events are available. Logical inferences from systematic observations, or even beliefs based on institutional experience may also be used. These data sources form the foundation for the probabilistic modeling and estimation of the relative frequency of adverse effects over time (Klinke, 2002).

The following descriptive analysis, derived from Bayes’ Theorem, allows one to represent the probability expression in (24), in a practical way; in terms of probabilities of occurrence, using likelihood data.

Consider first, from (49) and (50), that

$$P(\theta) \cdot P(\lambda | \theta) = P(\lambda) \cdot L(\theta | \lambda) \quad (69)$$

and from (52), as before, then

$$L(\theta | \lambda) = \frac{1}{P(\lambda)} \cdot P(\lambda | \theta) \quad (70)$$

It follows that the threat likelihood of each vulnerability is then given as

$$L_{s,i}(\theta | \lambda_{s,i}) = \frac{1}{P_{s,i}(\lambda)} \cdot P_{s,i}(\lambda_{s,i} | \theta, \delta_{s,i}) \quad (71)$$

$$= k \cdot P_{s,i}(\lambda_{s,i} | \theta, \delta_{s,i} = 0) \times P_{s,i}(\lambda_{s,i} | \theta, \delta_{s,i} = 1) \times \bar{E}_i \quad (72)$$

and hence, more generally as

$$L(\theta | \lambda) = k \cdot \prod_{N=1}^{n(\lambda)} P(\lambda_N | \theta, \delta) \quad (73)$$

However, for the threat likelihood of each IAS, this analysis forgoes the mathematical method, in the aggregation of probability distributions using

$$L_{n,s}(\theta | \lambda_{s,i}) = \prod_{N=1}^{n(L)} L_{s,i}(\theta | \lambda_{s,i}, \delta_{s,i}) \quad (74)$$

to instead adopt an axiomatic approach for combination, known as the linear opinion pool for PRA,

$$L_{n,s}(\theta | \lambda_{s,i}) = w_N \cdot \sum_{N=1}^{n(L)} L_{s,i}(\theta | \lambda_{s,i}, \delta_{s,i}) \quad (75)$$

where $n(L)$, represents the number likelihood values, and $n(\gamma)$, the number of vulnerabilities, also w_N , representing individual weights that sum to unity, within each IAS:

$$\sum_{N=1}^{n(L)} w_N = \frac{\omega_{s,i} + \dots + \omega_N}{\sum_N (\omega_{s,i} + \dots + \omega_N)} = 1 \quad (76)$$

Figures 8 through 15 illustrates the implementation of (73) through (76), providing perspective for the reader, the quantitative SRA of probabilities corresponding to the adverse events adopted from the DIACAP IAVM controls listed from Table 3. Likelihood values including corresponding impact coefficient values are taken from (Meritt, 1999) and incorporated into a probability-impact tree diagram for each of the ISS CIA risk dimensions.

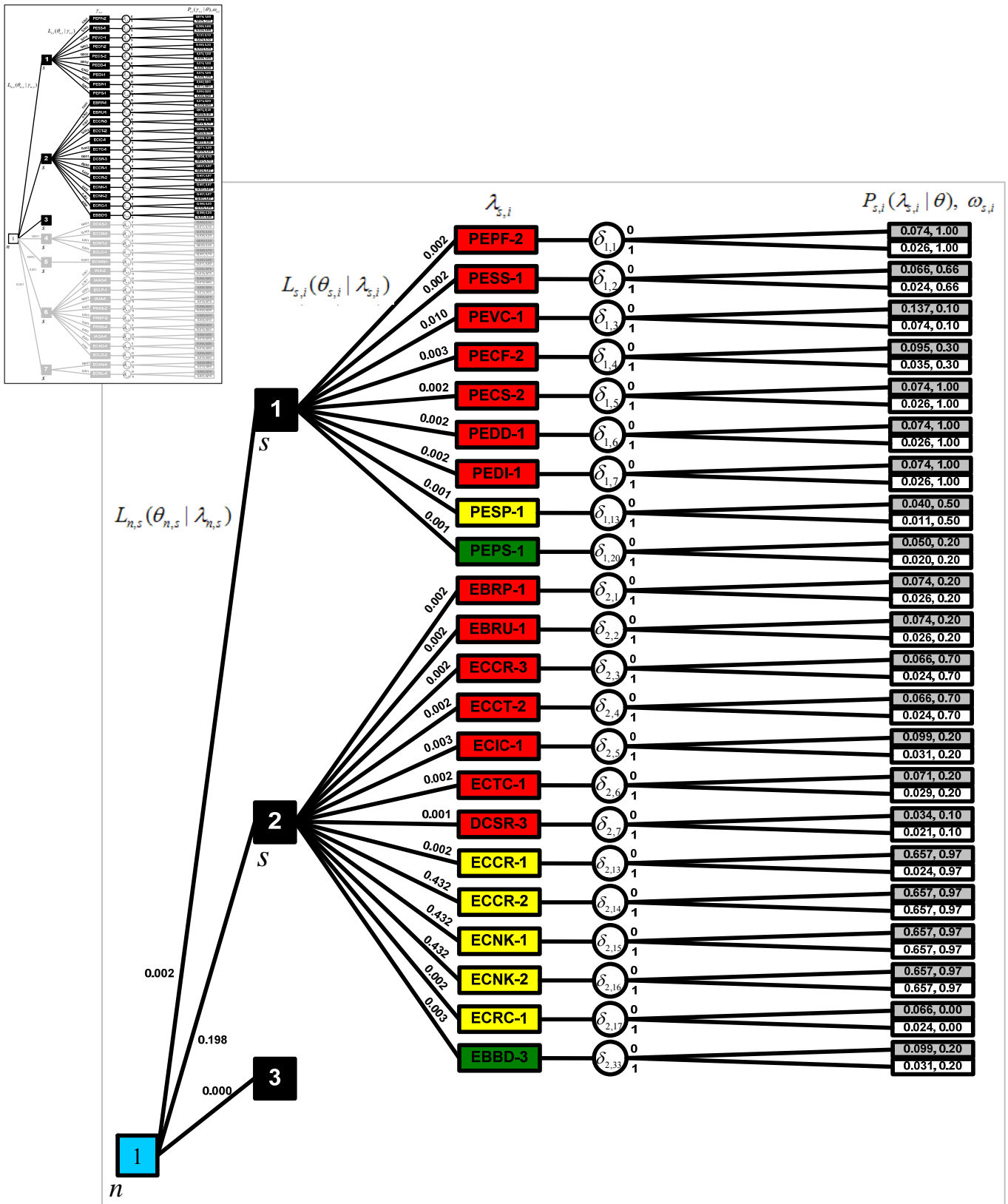


Figure 8. IAS (s = 1, 2, 3) Probability-Impact Tree Diagram for Confidentiality (n = 1)

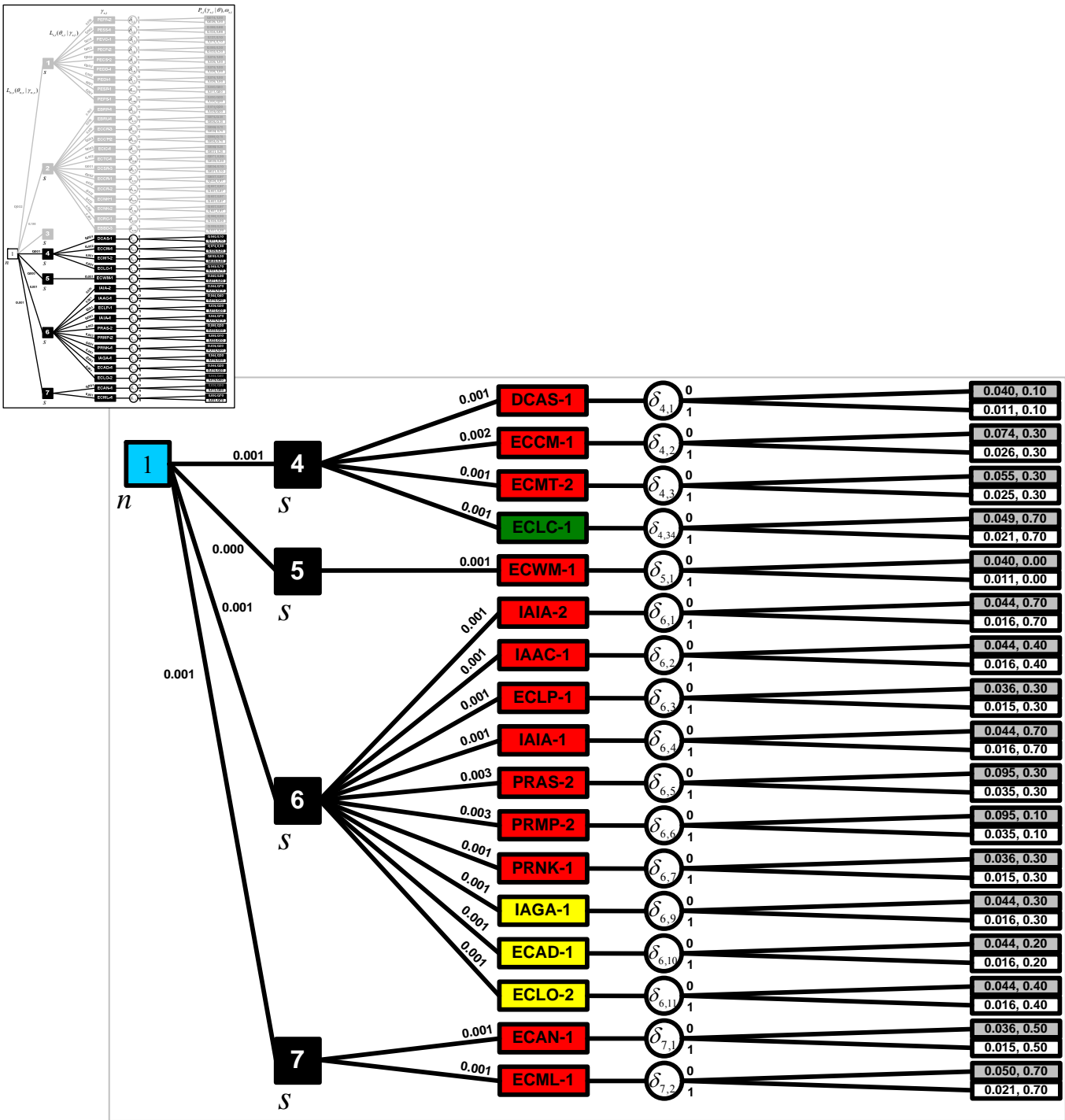


Figure 9. IAS ($s = 4, 5, 6, 7$) Probability-Impact Tree Diagram for Confidentiality ($n = 1$)

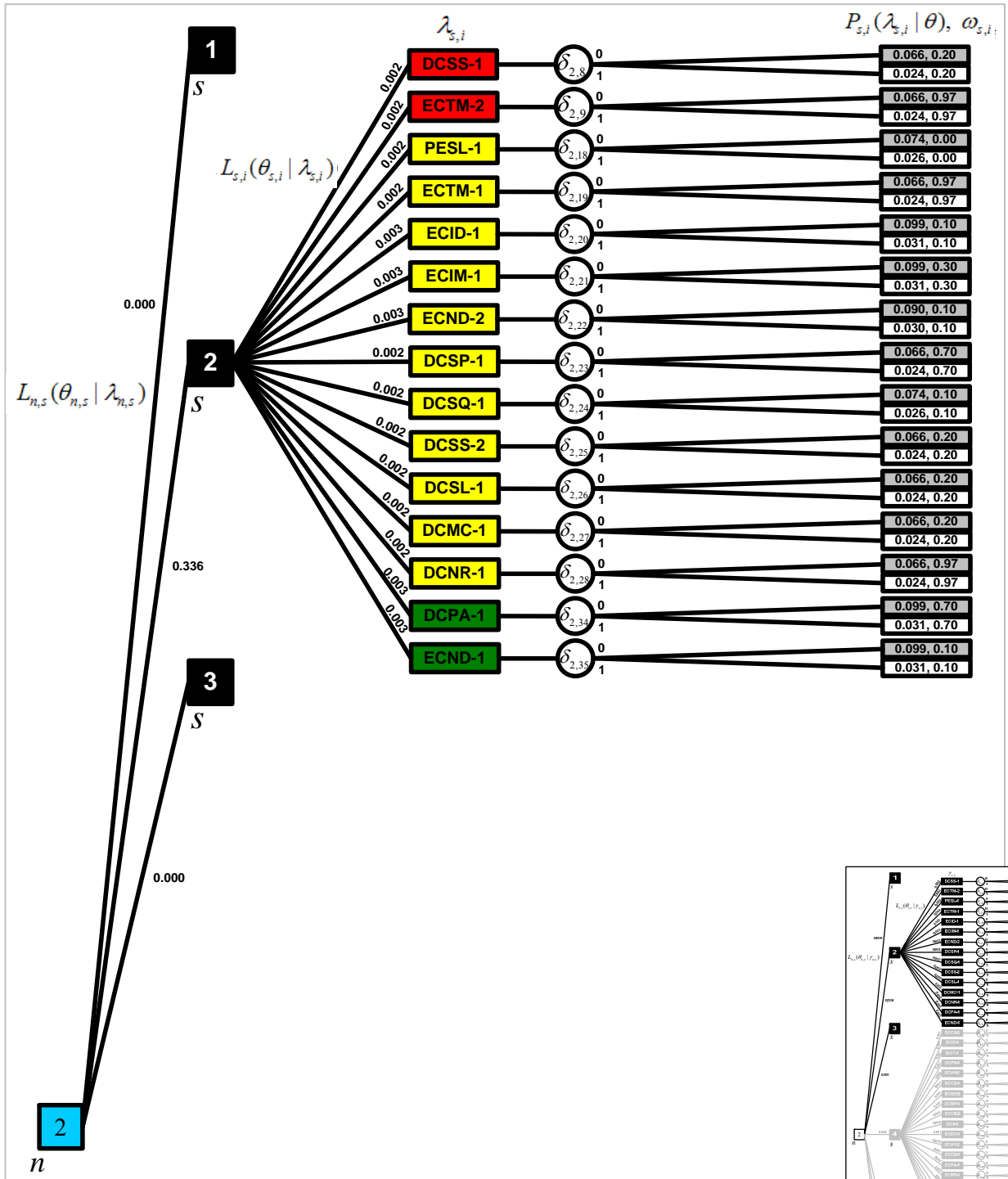
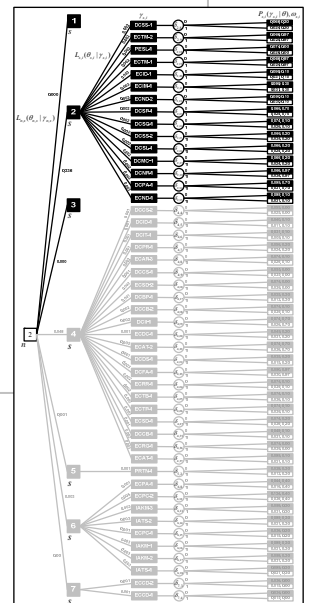


Figure 10. IAS ($s = 1, 2, 3$) Probability-Impact Tree Diagram for Integrity



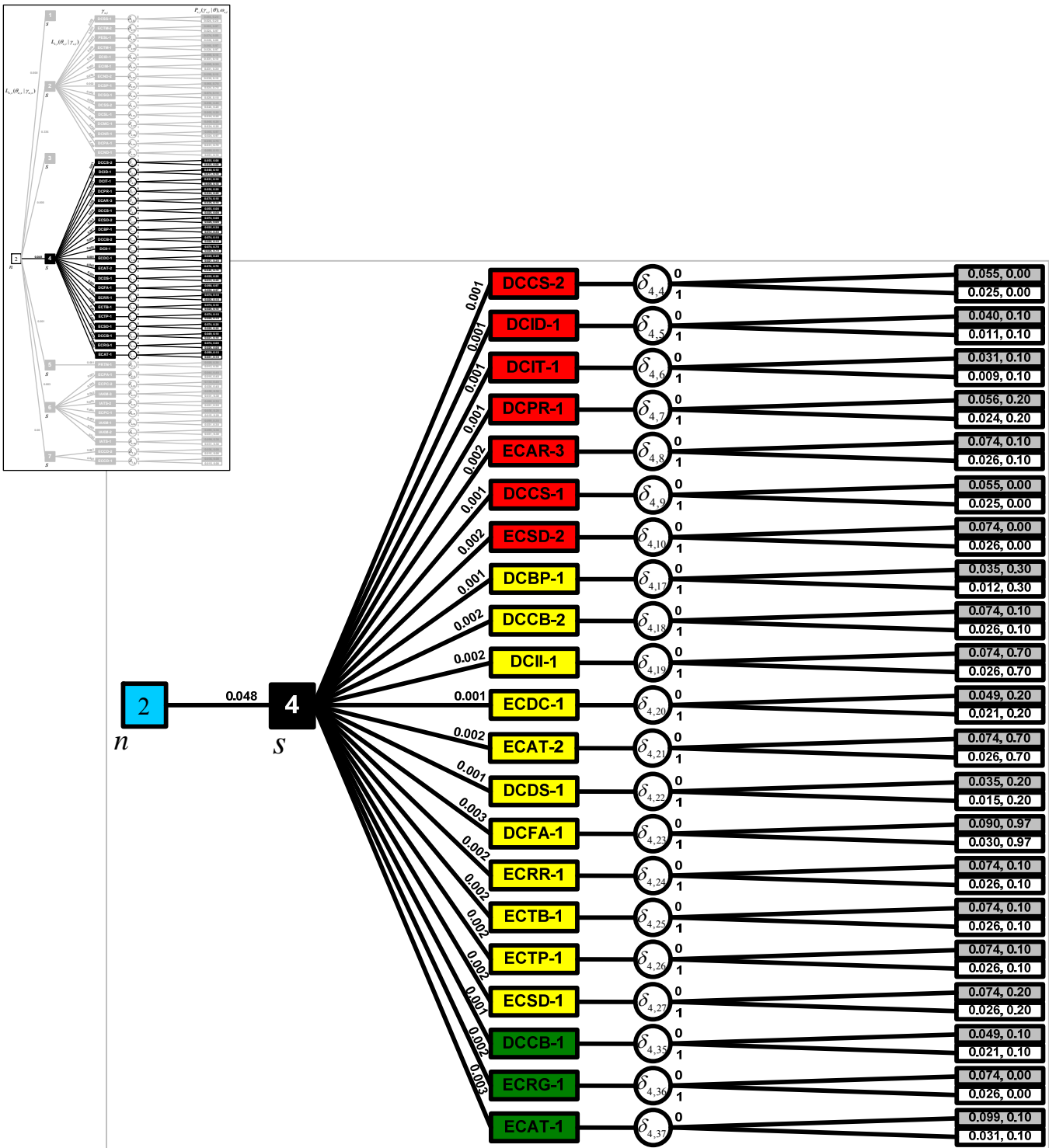


Figure 11. IAS ($s = 4$) Probability-Impact Tree Diagram for Integrity ($n = 2$)

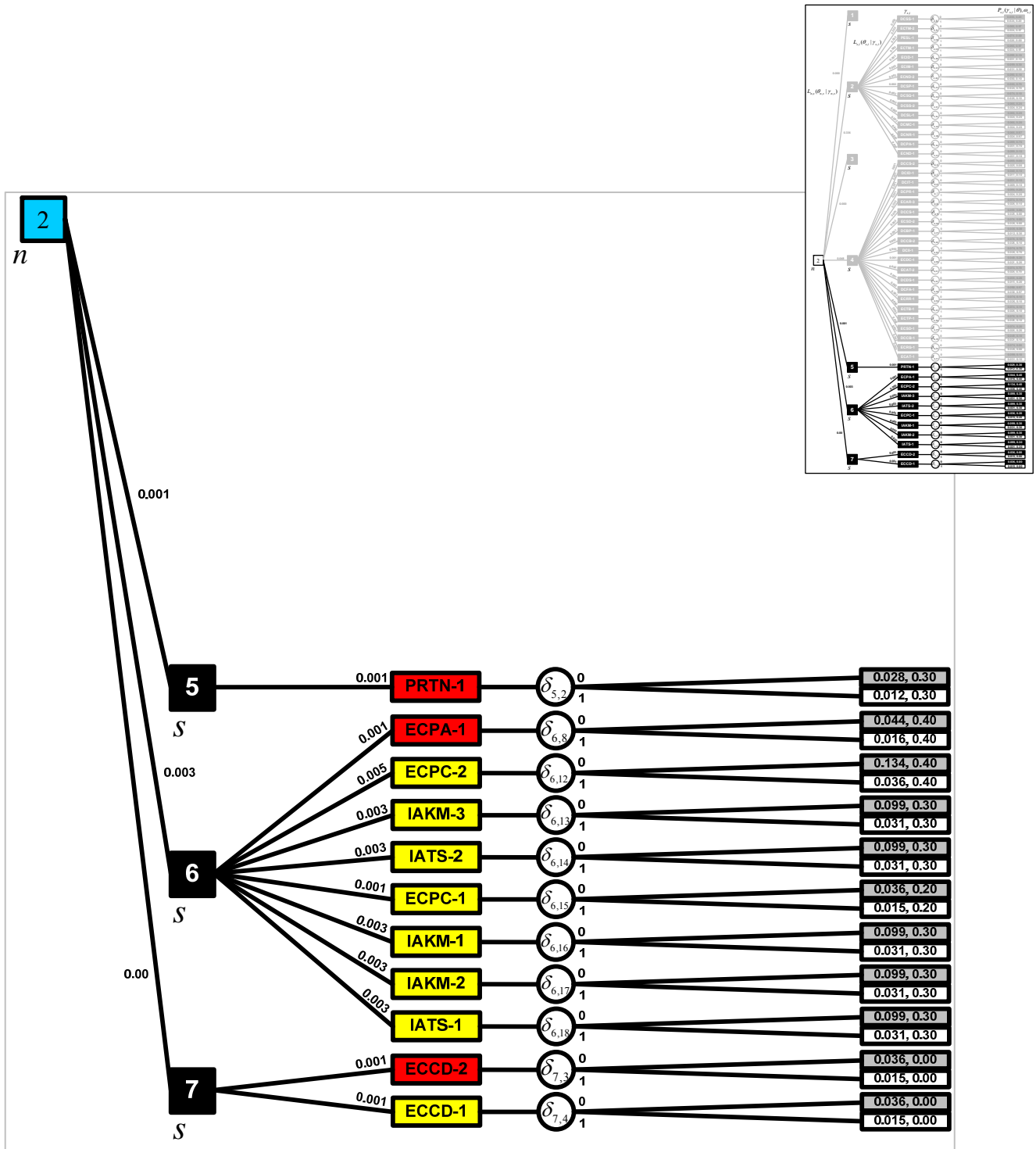


Figure 12. IAS ($s = 5, 6, 7$) Probability-Impact Tree Diagram for Integrity ($n = 2$)

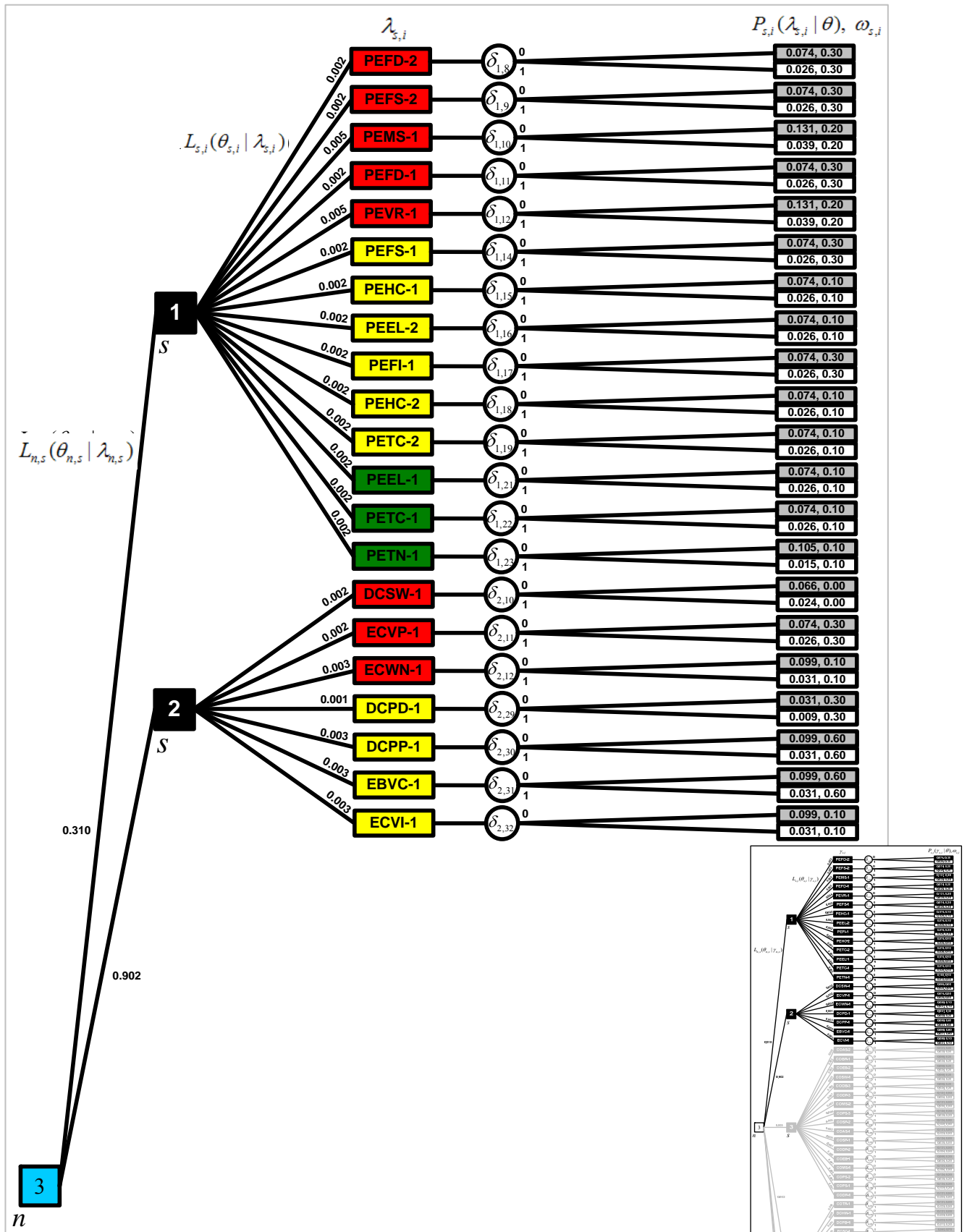


Figure 13. IAS ($s = 1, 2$) Probability-Impact Tree Diagram for Availability

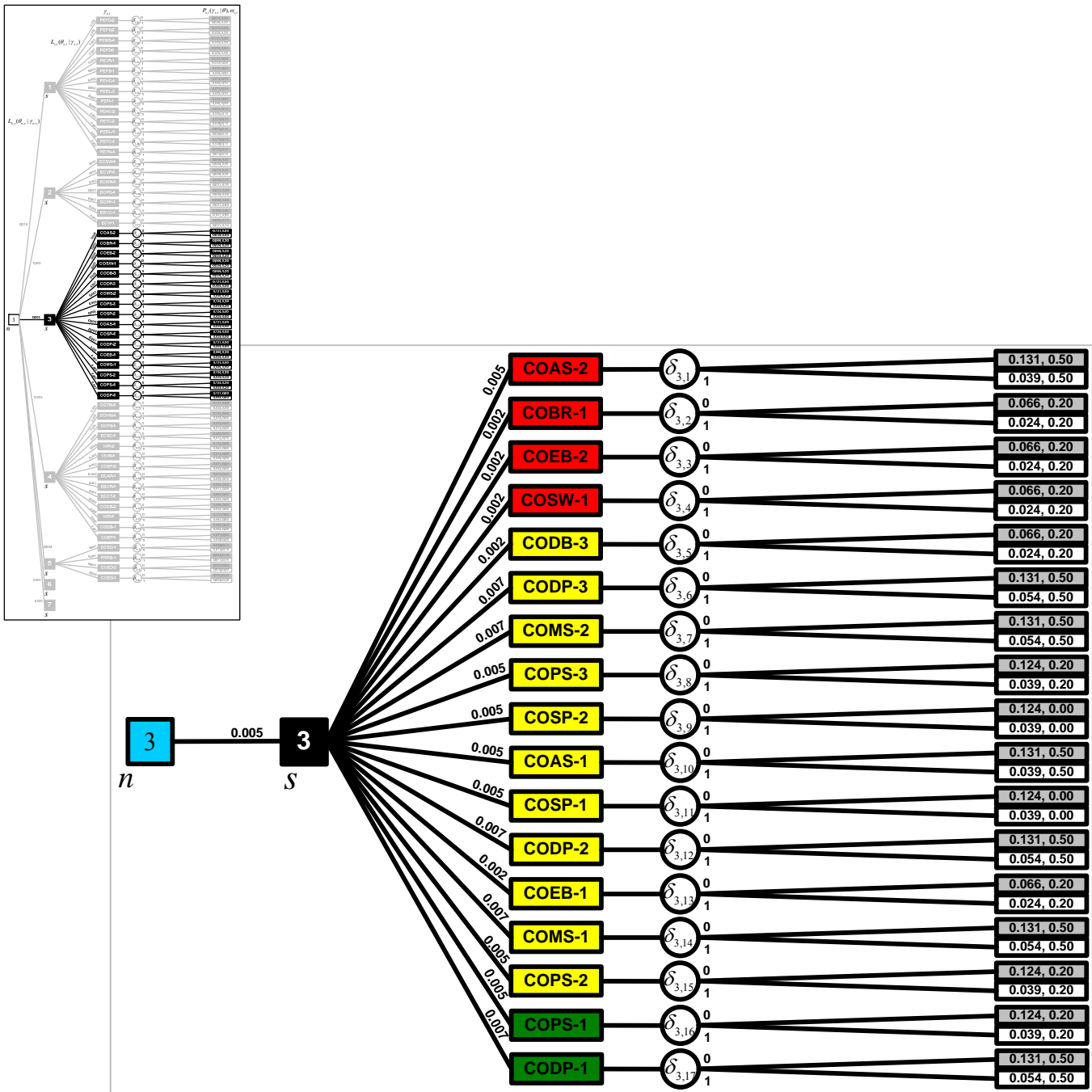


Figure 14. IAS ($s = 3$) Probability-Impact Tree Diagram for Availability ($n = 3$)

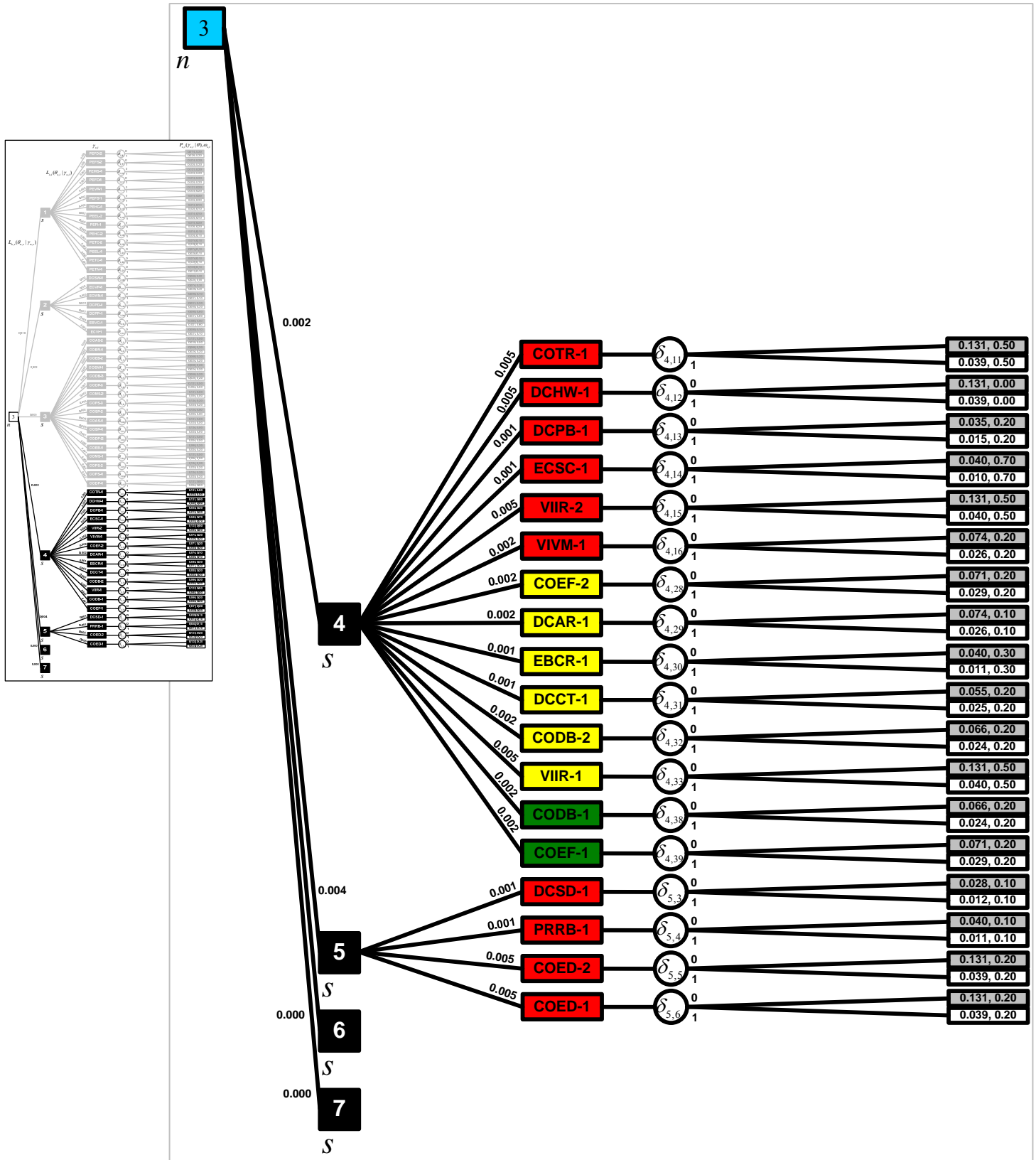


Figure 15. IAS ($s = 4, 5, 6, 7$) Probability-Impact Tree Diagram for Availability ($n = 3$)

Reliability

While the subject of statistics is considered to be a science in the handling of data, the scope and focus of this paper relies on probability, as a science concerned with the handling of a lack of data. Although non-significant results (within one standard deviation) from a general comparison can be made, the concern is not, so much as to see, how closely quantitative values match up with qualitative ones, but instead to analyze the behavior and sensitivity of both a time-dependent and independent quantitative risk expression for CIS. It's the examination of the SRA approach itself; the exercise in the use of such an expression using test models, combined with the understanding its viability and meaningfulness that is most important to the general subject of risk and those whom seek to adopt a SRA approach to CIS.

Of course, the reliability of this analysis is only as good as the reliability of the probability data used, thus, arriving at the source of this paper's primary research question (RQ1), and the greatest weakness in the application of a quantitative SRA approach. This is particularly important in risk analyses, where the fundamental input data on exploit rates of CIS components is uncertain. Chapter 2, and the Problem Breakdown section (within pages 16 and 17), have provided the reader with a sufficient background of the challenges and difficulty resulting from the scarcity of reliable data for information systems, let alone, for CIS.

As aware as the problem has become, this paper has been able to successfully identify and adopt two reliable sources of probability data from (i) the United States Computer Emergency Readiness Team (US-CERT) Threat and Vulnerability Database, and (ii) a combination from the National Institute of Standards & Technology (NIST) Computer

Security Resource Center (CSRC) National Information Systems Security Conference (NISSC), and the CSO Magazine 2006 E-Crime Watch Survey, U.S. Secret Service, CERT Coordination Center, Microsoft Corp. (CERT.org, 2006), with the latter used to implement Bayes' Theorem and provide for a Probability-Impact Tree for each of the ISS risk dimensions. Although, the impact coefficient values, from the NISSC whitepaper, were derived using the combined experience and skills of a number of experts in the arena of information systems security, they are understood, ultimately to be only suggested values (Meritt, 1999). The 2006 E-Crime Watch Survey was deployed to 15,000 readers, comprising of security and law enforcement professionals, yielding 434 respondents, and having a +/- 3.4% margin of error (CERT.org, 2006).

Data from NISSC, used to illustrate the application of Bayes' Theorem, is intuitively more reliable towards its use in a time-independent, quantitative risk expression, rather than data from the US-CERT Threat and Vulnerability database, which has tracked its data over the past several years, making it more suited for use in a time-dependent, quantitative risk expression. For analysis, the US-CERT Vulnerability and Threat Incident data plots, in Figures 5 and 6, quadratically regressed in (47) and (48) respectively, are used in conjunction with the Likelihood Function, given by,

$$L(\theta | \lambda) = \left(\frac{\lambda(t)^{\theta(t)}}{\theta(t)!} \right) \cdot e^{-\lambda(t)} \quad (77)$$

and picking up from (49) through (52), it follows that,

$$P_{n,s}(\lambda | \theta) \propto P(\lambda) \cdot \left(\frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t)+1]} \right) \cdot e^{-\lambda(t)} \quad (78)$$

Security Risk Analysis

Research Question 1 (RQ1).

Is it possible to create a meaningful continuous, time-dependent, quantitative risk expression for CIS given existing security risk analysis (SRA) techniques?

Results

Recall, from (43), a continuous, time-dependent, quantitative risk expression is presented for the SRA of CIS as,

$$R_{s,i}(t) = \int_{t_1}^{t_2} \left\{ 1 - \left[P_{s,i}(\lambda) \cdot \left(\frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t)+1]} \right) \cdot e^{-\lambda(t)} \right] \cdot [1 - \delta_{s,i}(t)] \right\} \cdot \left\{ \omega_{s,i} \cdot [1 - \gamma(\delta_{s,i}, t)] \right\} dt \quad (79)$$

given (78), (47), (48), (26), and (31), where

$$\lambda(t) = (73)t^2 - (2.9 \cdot 10^5)t + (2.9 \cdot 10^8) \quad (47)$$

$$\theta(t) = (4.5 \cdot 10^3)t^2 - (1.8 \cdot 10^7)t + (1.8 \cdot 10^{10}) \quad (48)$$

$$\delta_{s,i} = \begin{cases} 0, & \text{iff Non-Compliant (NC)} \\ 1, & \text{if Compliant (C) } \oplus \text{ Not Applicable (N/A)} \end{cases} \quad (26)$$

$$\omega_{s,i} = \frac{1}{100} \left(1 - \left| -12.5\omega_{\text{CAT}}^2 + 67.5\omega_{\text{CAT}} - 95 \right| \right) \quad (31)$$

$$\omega_{\text{CAT}} = \begin{cases} 1, & \text{if CAT I} \\ 2, & \text{if CAT II} \\ 3, & \text{if CAT III} \end{cases} \quad (80)$$

$$0 \leq \gamma(\delta_{s,i}, t) \leq 1 \quad (81)$$

The sensitivity and multivariate analysis of (79) is divided up and presented to the reader by parts, starting with (i) the Likelihood Function, and its product with the, (ii) effectiveness of the control; (iii) the impact factor, and its product with, (iv) confidence factor adjustments; with (v) the entire product of (i) through (iv), subtracted from unity, (vi) the effect of integration between, Δt , and finally, (vii) resulting risk values, analyzed for consistency with values aligning with the expected behavior, and interpretation of the adopted unit of measurement, as described in the descriptive statistics section of this chapter.

Given Vulnerability and Threat expressions, from (47) and (48), the Likelihood Function in (78) is expanded as

$$P^* \propto P(\lambda) \cdot \left[\frac{\left(73t^2 - 2.9 \cdot 10^5 t + 2.9 \cdot 10^8\right)^{4500(t-2000)^2}}{\Gamma\left(4.5 \cdot 10^3 t^2 - 1.8 \cdot 10^7 t + 1.8 \cdot 10^7\right)} \right] \cdot e^{-73t^2 + 2.9 \cdot 10^5 t - 2.9 \cdot 10^8} \quad (82)$$

A cursory review reveals several issues, assuming we are looking at resulting likelihood values between the time frame of 2010 through 2020, in the calculation of an expression involving such high magnitudes of power. For example, (i) both the gamma function in the denominator, and exponential in the numerator, each approach infinity easily, leading to a result too large to represent as a conventional floating-point value, and (ii) with the negative exponential, on the right, reaching asymptotic zero fairly quickly. This does not render the expression in (82) completely meaningless, but instead, simply requires that the behavior be expressed in a way that is manageable for our application.

Dividing the entire expression in (82) by the highest numerical value, $1.8 \cdot 10^7$, and encapsulating the result within an arctangent function, preserves the unity constraint established for (79), while maintaining the behavioral integrity of the Likelihood function:

$$P^* \propto P(\lambda) \cdot \left[\frac{2}{\pi} \cdot \arctan \left(2\pi \cdot \frac{\left(\frac{73}{18000000} t^2 - \frac{29}{1800} t + \frac{145}{9} \right)^{1/4000(t-2000)^2}}{\Gamma\left(\frac{1}{4000} t^2 - t + 1001\right)} \right) \right] \cdot e^{\frac{-73}{18000000} t^2 + \frac{29}{1800} t - \frac{145}{9}} \quad (83)$$

Given the modified function in (83), which is based on the Vulnerability and Threat Incident figures detailed by US-CERT, the coefficient values for the conditional probability of an attack for the years beginning from 2010 and ending through 2020 are calculated and listed within the table below. Outliner values 1 and 9999, for t , are also included for analysis of sensitivity.

Table 6

Coefficient Values for the Conditional Probability of an Attack

Year (t)	$\lambda^*(t)$	$\theta^*(t)$	$L(\theta \lambda)$	$P^* / P(\lambda)$
1	16.0950	999.003	--	--
2010	0.1126	0.0250	0.8124	0.8768
2011	0.1128	0.0302	0.8122	0.8768
2012	0.1130	0.0360	0.8121	0.8768
2013	0.1132	0.0423	0.8119	0.8768
2014	0.1135	0.0490	0.8117	0.8767
2015	0.1137	0.0563	0.8115	0.8767
2016	0.1139	0.0640	0.8113	0.8767
2017	0.1142	0.0722	0.8111	0.8767
2018	0.1144	0.0810	0.8109	0.8766
2019	0.1147	0.0902	0.8107	0.8766
2020	0.1150	0.1000	0.8105	0.8766
9999	260.4906	15996	--	--

Note the increasing number of predicted vulnerabilities, and associated threat incidents as time increases, while the conditional likelihood of an increasing threat dynamic acting on an increasing vulnerability count remains approximately constant, even slightly, dropping ten-thousandth of a percentage annually.

As expressed in (25) through (27), the effectiveness value of a control is essentially binary, as the control is either being implemented, within compliance, $\delta_{s,i} = 1$, or not, $\delta_{s,i} = 0$. This is a qualitative concept. Some controls for vulnerabilities, such as the installation of up-to-date patches, required for proper patch management, or the backup of critical data, requires weekly and/or even daily sustainment by a system administrator. Quantitatively this risk element, expressed as a continuous function $\delta_{s,i}(t)$, and the effectiveness value of the control can, in fact, be modeled for growth or decay as time passes. The modeling of such behavior for this risk element is in line with a quantitative SRA approach. Current tools like VMS (Vulnerability Management System) track compliance resulting in the binary risk assessment of the control over time, however, whether this is considered a completely quantitative approach is up for debate. The results of system scans uploaded to VMS provides open, closed, and total findings; when incorporated into a metric may be considered quantitative.

A continuous 3-point quadratically regressed function, designated as an impact factor, $\omega_{s,i}$, was calculated and expressed in (31), from a risk assessment approach currently being adopted for CIS at a CC/S/A. The modeling of this risk element is organizationally dependent and must take into account the negative consequence or impact to the organization. Each IA DIACAP vulnerability listed within the DoDI 8500.2, Controls for Classified Systems, Table 3, has a qualitative-based, Category (CAT) level assigned to it that corresponds directly to a qualitative impact value for scoring adjustments, as seen in Table 1. In approaching a comparison of both qualitative and quantitative SRA, the impact-coefficients values derived from (Meritt, 1999) and (CERT.org, 2006) are used, in place of the standardized CAT levels and associated impact factor adjustments for each of the vulnerabilities.

The confidence factor, γ , is formally introduced and defined as (23), with its continuous behavior elaborated on within the Assumptions Section of (on page 23). The effectiveness of a confidence factor has an unique relationship to impact, similar to that seen with the effectiveness of a control to the conditional probability of a compromise/attack. Besides the passing of time, a confidence factor can also have dependence on the behavior and effectiveness of a control; hence a function of two variables, $\gamma(\delta_{s,i}, t)$.

In order for the quantitative risk expression in (79) to maintain its meaningfulness, all its elements must mathematically behave within the resultant boundary of unity, (0,1]. In addition, the subsequent product of each risk component, Ω_c , within the expression, must align with a behavior that maintains consistency with the intended meaning of its results. The following truth table below validates such behavior.

Table 7

Truth Table for the Component Behavior of a Quantitative Risk Expression

Component	Description	$\Omega_c \rightarrow 0$	$\Omega_c \rightarrow 1$
$P(\lambda)$	Probability of Vulnerability	$R_{EV} \rightarrow 1$	X
$P^* / P(\lambda)$	Likelihood Function	$R_{EV} \rightarrow 1$	X
ω	Impact Factor	$R_{EV} \rightarrow 1$	X
$[1 - \delta(t)]$	Control Effectiveness	$R_{EV} \rightarrow 1$	X
$[1 - \gamma(\delta, t)]$	Confidence Effectiveness	$R_{EV} \rightarrow 1$	X
R_{EV}	Risk, Expected Value	HIGH RISK, $R_{LC} \rightarrow 1$	LOW RISK, $R_{LC} \rightarrow 0$
R_{LC}	Risk, Loss Confidence	LOW LOSS	HIGH LOSS

CIS Test Model: **01/Y**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
100%	100%	100%	100%	100%	100%	100%	100%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~100%	~100%	~100%	~100%

Figure 16. Analysis: Note that, unless a qualitative appraisal score of 100% has no impact/consequence, such a score violates the quantitative SRA rule of (65).

CIS Test Model: **02/CQRSTUVWIJKP**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
100%	100%	100%	100%	100%	100%	100%	100%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~100%	~100%	~100%	~100%

Figure 17. Analysis: This model contains at least a single confidence adjustment in every IAS.

CIS Test Model: **22/CQRSTUIJK**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
95%	95%	95%	95%	95%	100%	100%	95%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
31.9%	38.6%	69.7%	46.7%

Figure 18. Analysis: The qualitative scorecard for this CIS Test Model contains a non-compliant CAT III finding in all but 2 IAS. The following five controls were selected: PEPS-1, DCPA-1, COPS-1, ECLC-1, COED-1 spanning all three ISS.

CIS Test Model: **40/BQRSTUUVWIJK**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
90%	90%	90%	90%	90%	90%	90%	90%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
58.8%	69.1%	69.7%	65.9%

Figure 19. Analysis: Model containing NC CAT II findings: PESP-1, PESL-1, DCCB-2, IAKM-1, COED-2, ECCD-1; spanning all ISS, & revealing a 24% delta between score totals.

CIS Test Model: **62/AQRSTUUVWIJK**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
60%	60%	60%	60%	60%	60%	60%	60%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
10.3%	51.4%	58.8%	40.2%

Figure 20. Analysis: Test Model containing NC CAT I findings: PEPF-2, ECWM-1, ECAN-1, DCSS-1, DCIT-1, ECPA-1, COAS-2; spanning all ISS, & revealing a 20% delta score.

CIS Test Model: **74/BCQRSTUJ**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
95%	95%	95%	95%	95%	100%	90%	90%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
83.5%	42.3%	58.2%	61.3%

Figure 21. Analysis: Test Model containing NC CAT II and CAT III findings: PEPS-1, DCPA-1, ECCD-1, COPS-1, CODB-1, COED-1 showing a 29% delta between score totals.

CIS Test Model: **90/ABQRSTUVWJ**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
90%	90%	90%	90%	90%	90%	60%	60%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
82.5%	83.2%	56.1%	73.9%

Figure 22. Analysis: Test Model containing NC CAT I and CAT II findings: ECAD-1, ECID-1, ECCD-2, PEEL-2, CODB-3, VIIR-1, COED-2 showing a 14% delta between score totals.

CIS Test Model: **91/BCQRSTUVWIJKP**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
60%	60%	60%	60%	60%	60%	60%	60%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
4.3%	73.7%	56.2%	44.7%

Figure 23. Analysis: Test Model contains at least a single confidence adjustment and at least two NC findings per IAS: PEPF-2, PESS-1, DCAS-1, ECCM-1, IAIA-2, IAAC-1, ECCD-2, DCSS-1, ECTM-2, PRTN-1, ECCD-1, COAS-2, COBR-1, DCSD-1 showing a 15% delta between score totals.

CIS Test Model: **92/BCQRSTUVWIJKXP**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
50%	50%	50%	50%	50%	50%	50%	50%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
3.2%	55.3%	42.2%	33.6%

Figure 24. Analysis: PEPF-2, PESS-1, DCAS-1, ECCM-1, IAIA-2, IAAC-1, ECCD-2, DCSS-1, ECTM-2, PRTN-1, ECCD-1, COAS-2, COBR-1, DCSD-1 showing a 12% delta between score totals. Half of the controls have a 75% confidence weighting.

CIS Test Model: **93/CQRSTUVWIJK**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
85%	85%	90%	70%	95%	100%	100%	70%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
7.8%	29.3%	21.6%	19.6%

Figure 25. Analysis: Test Model containing multiple NC CAT III finding per IAS: PEPS-1, EBBD-3, ECLC-1, DCPA-1, ECND-1, DCCB-1, ECRG-1, ECAT-1, PEEL-1, PETC-1, COPS-1, CODP-1, CODB-1, COEF-1, COED-1 showing a 50% delta between score totals.

CIS Test Model: **96/CQRSTUVWK**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
85%	70%	90%	70%	95%	100%	100%	70%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
7.8%	8.35%	21.6%	12.6%

Figure 26. Analysis: PEPS-1, EBBD-3, ECLC-1, DCPA-1, ECND-1, DCCB-1, ECRG-1, ECAT-1, PEEL-1, PETC-1, COPS-1, CODP-1, CODB-1, COEF-1, COED-1, ECIM-1, COPS-1 showing a 57% delta between score totals.

CIS Test Model: **97/BQRSTUVWIJKX**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
30%	-100%	-10%	-70%	90%	0%	90%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
0.01%	~0%	1.0%	0.3%

Figure 27. Analysis: Test Model containing maximum number of NC MAC II findings for all IAS. Note that this is an extreme case with a negligible delta between score totals.

CIS Test Model: **98/BQRSTUUVWIX**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
90%	50%	100%	100%	100%	70%	100%	50%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
0.0%	~100%	~100%	66.7%

Figure 28. Analysis: : Test Model containing NC MAC II findings with an individual qualitative IAS score below <60%. Vulnerabilities affecting Confidentiality ISS only.

CIS Test Model: **99/BQRSTUUVWJX**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
100%	-10%	100%	-10%	100%	30%	90%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~100%	~0%	~100%	66.7%

Figure 29. Analysis: Test Model containing NC MAC II findings with an individual qualitative IAS score below <60%. Vulnerabilities affecting Integrity ISS only.

CIS Test Model: **100/BQRSTUUVWKX**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
40%	60%	-10%	40%	90%	100%	100%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~100%	~100%	~0%	66.7%

Figure 30. Analysis: Test Model containing NC MAC II findings with an individual qualitative IAS score below <60%. Vulnerabilities affecting Availability ISS only.

CIS Test Model: **101/AQRSTUVWIJKX**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
-380%	-380%	-60%	-540%	-60%	-220%	-20%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~0%	~0%	~0%	~0%

Figure 31. Analysis: Test Model containing NC MAC I finding with an individual qualitative IAS score below <60%. Vulnerabilities affecting all IAS only.

CIS Test Model: **102/AQRSTUVWI**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
-280%	-280%	100%	-20%	60%	-180%	20%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~0%	~100%	~100%	66.7%

Figure 32. Analysis: Test Model containing NC MAC I finding with an individual qualitative IAS score below <60%. Vulnerabilities affecting Confidentiality ISS only.

CIS Test Model: **103/AQRSTUVWJX**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
100%	20%	100%	-180%	60%	60%	60%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~100%	~0%	~100%	66.7%

Figure 33. Analysis: Test Model containing NC MAC I finding with an individual qualitative IAS score below <60%. Vulnerabilities affecting Integrity ISS only.

CIS Test Model: **104/AQRSTUVWKX**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
-100%	-20%	-60%	-140%	20%	100%	100%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~100%	~100%	~0%	66.7%

Figure 34. Analysis: Test Model containing NC MAC I finding with an individual qualitative IAS score below <60%. Vulnerabilities affecting Availability ISS only.

CIS Test Model: **106/Z**

QUALITATIVE RESULTS: INFORMATION ASSURANCE SERVICE (IAS), s							TOTAL
1	2	3	4	5	6	7	
-470%	-595%	-180%	-740%	-75%	-320%	-30%	0%

QUANTITATIVE RESULTS: INFORMATION SECURITY SERVICE (ISS), n			TOTAL
1	2	3	
~0%	~0%	~0%	~0%

Figure 35. Analysis: Maximum NC Findings for all vulnerabilities revealing individual negative IAS scores. Note that the quantitative results avoids this ambiguity.

Figures 16-36 provide the reader a basic comparison between Qualitative and Quantitative SRA results for special selected cases, from the developed pool of CIS Test Models, listed within Table 5. Although a comprehensive comparison between the two totals would not yield a significant conclusion to take away from, it does satisfy RQ1, in that the mechanics of a quantitative expression does follow the general behavior of a qualitative one, and that a meaningful continuous, time-dependent, quantitative risk expression for CIS, not only can be created, but applied. The results reveal similar behavior between the appraisal of IAS and ISS, with qualitative ISS result totals averaging slightly below IAS totals.

Research Question 2 (RQ2).

Is it possible to create a meaningful, continuous, time-dependent, quantitative risk determination metric for CIS from a risk expression?

Results

The second component to this thesis is the presentation, and meaningful interpretation, of a risk determination metric for the SRA of CIS: a measurement framework by which CC/S/A's may adopt in the evaluation and determination of risk acceptability. Exploration of RQ2 offers insight into the perennial question on "What is considered risk acceptable?" It is important to realize that the difficulty lies, in the fact, that risks are not linearly comparable, unless, functional risk elements, that are organizationally and CIS dependent, such as impact models, are assumed compatible to those risks by which are being compared.

Secondly, there is difficulty with the notion of acceptable risk, in that, risk cannot be spoken of as acceptable or not, in isolation, but only in combination with the costs, and merits that are associated with that risk. One needs to adopt a decision theory point of view, with the optimum mix of cost and benefit with risk selection. Nothing is without risk and risk is always compared against operational benefit and cost (Cieslak, 2009). A cost-benefit involves the consideration of whether, or not, risks should be reduced with costs; usually characterized in monetary terms, as fundamentally determined by the definitions expressed in (1) through (4).

Considered in isolation, no risk is acceptable (Kaplan, 1981). If a given risk is determined to be unacceptable, adequate measures for risk reduction are required; a common process within the domain of 'risk management'. Since the number of risks associated with CIS exceeds, both the scope of this paper and the SRA by InfoSec analysts, the conventional

risk management solution has been to create a combination, between the setting of risk priorities by severity, and the magnitude of potential effects those risks may have. This proportional, risk-risk comparison, constitutes the priority instrument for today's risk management approach.

It is management's responsibility to set their level of risk. Each organization has its own acceptable risk level, derived from legal and regulatory compliance responsibilities, its threat profile, and mission impact. The purpose in addressing RQ2 is to contribute to the understanding of a risk acceptance level and risk criteria for CIS. The first consideration involves the setting of boundary curves for risk acceptance, in part by, the characteristics and limitations examined from the analysis in RQ1.

Recall from (45), that a continuous, time-dependent, quantitative risk determination expression presented for the SRA of CIS is given as,

$$D(R) = R_{s,i}(t) \cdot \frac{dR_{s,i}(t)}{dt} \cdot \frac{d^2R_{s,i}(t)}{dt^2} \quad (84)$$

where

$$R_{s,i}(t) = \int_{t_1}^{t_2} \left\{ 1 - \left[P_{s,i}(\lambda) \cdot \frac{2}{\pi} \cdot \arctan \left(2\pi \cdot \frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t)+1]} \right) \cdot e^{-\lambda(t)} \right] \cdot [1 - \delta_{s,i}(t)] \right\} \cdot \{ \omega_{s,i} \cdot [1 - \gamma(\delta_{s,i}, t)] \} dt \quad (85)$$

As previously discussed, the expected value in (84) is time-dependent, taking into account both the rate of risk and risk variability. Assuming, for the purpose of illustrating the validating of the behavior in (84), assigning the set of risk components, Ω_{sc} ,

$$\Omega_{sc} \in \{ P_{s,i}(\lambda), \omega_{s,i}, [1 - \delta_{s,i}(t)], [1 - \gamma(\delta_{s,i}, t)] \} \quad (86)$$

to unity

$$\Omega_{sc} = 1 \tag{87}$$

simplifying the risk expression in (79), and yielding the following maximum impact risk expression:

$$R_{s,i}(t) = \int_{t_1}^{t_2} \left(\frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t)+1]} \cdot e^{-\lambda(t)} \right) dt \tag{88}$$

By substituting (88) into the risk determination expression in (84), the following graph and corresponding expression in (89), for the maximum risk boundary curve, $D[R_{EV}(t)]$ is attained

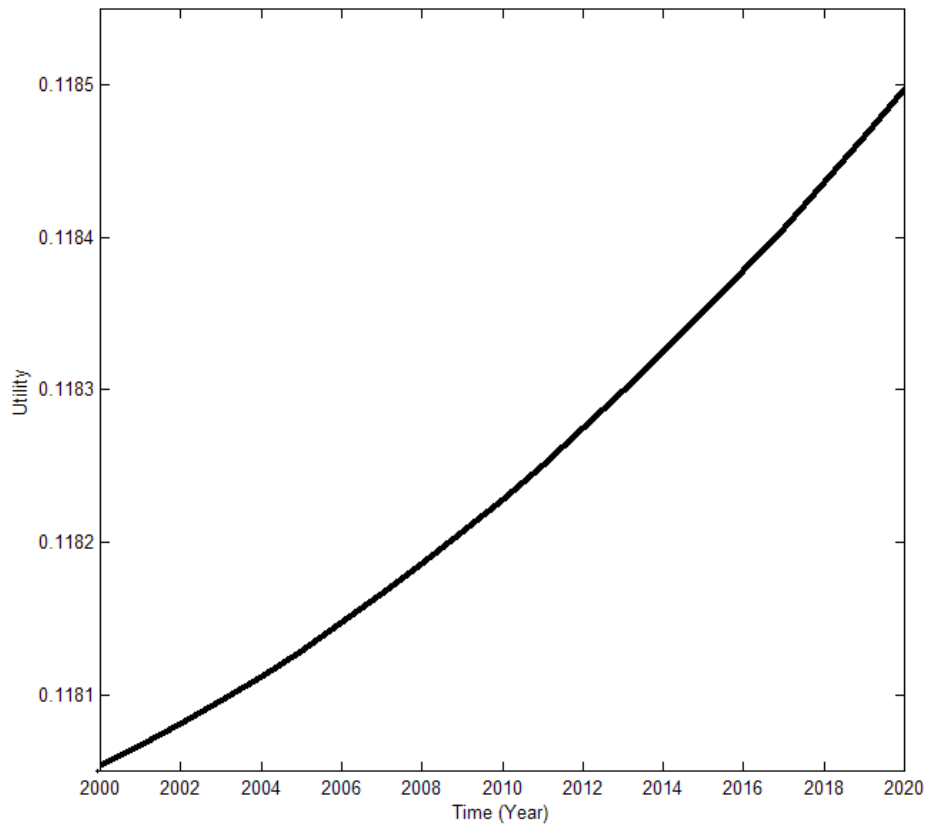


Figure 36. Risk Determination Curve: Maximum Boundary Over Time

$$\begin{aligned}
 & \left(\frac{\%4 \%6 \%1}{\%2} - \frac{\%4 \%1 \%5 (1/2000 t - 1)}{\%2} + \frac{\%4 \left(-\frac{73}{9000000} t + \frac{29}{1800} \right) \%1}{\%2} \right) \left(\frac{1/2000 t - 1}{\%3} \right) \\
 & + \frac{\%4 \%6^2 \%1}{\%2} + \%4 \left(\frac{1/2000 \log(\%3) + 2}{\%3} \frac{(1/2000 t - 1) \left(-\frac{73}{9000000} t - \frac{29}{1800} \right)}{\%3} \right) \\
 & + \frac{73}{9000000} \frac{1/4000 t^2 - t + 1000}{\%3} \\
 & - \frac{(1/4000 t^2 - t + 1000) \left(-\frac{73}{9000000} t - \frac{29}{1800} \right)^2}{\%3^2} \%1/\%2 \\
 & - 2 \frac{\%4 \%6 \%1 \%5 (1/2000 t - 1)}{\%2} + 2 \frac{\%4 \%6 \left(-\frac{73}{9000000} t + \frac{29}{1800} \right) \%1}{\%2} \\
 & + \frac{\%4 \%1 \%5^2 (1/2000 t - 1)^2}{\%2} \\
 & - 2 \frac{\%4 \left(-\frac{73}{9000000} t + \frac{29}{1800} \right) \%1 \%5 (1/2000 t - 1)}{\%2} \\
 & - \frac{\%4 \%1 \Psi(1, 1/4000 t^2 - t + 1001) (1/2000 t - 1)^2}{\%2} \\
 & - 1/2000 \frac{\%4 \%1 \%5}{\%2} - \frac{73}{9000000} \frac{\%4 \%1}{\%2} + \frac{\%4 \left(-\frac{73}{9000000} t + \frac{29}{1800} \right)^2 \%1}{\%2} \Big/ \%2 \\
 \\
 \%1 & := \exp\left(-\frac{73}{18000000} t^2 + \frac{29}{1800} t - 145/9\right) \\
 \%2 & := \text{gamma}(1/4000 t^2 - t + 1001) \\
 \%3 & := \frac{73}{18000000} t^2 - \frac{29}{1800} t + 145/9 \\
 \%4 & := \%3^2 \\
 \%5 & := \Psi(1/4000 t^2 - t + 1001) \\
 \%6 & := (1/2000 t - 1) \log(\%3) + \frac{(1/4000 t^2 - t + 1000) \left(-\frac{73}{9000000} t - \frac{29}{1800} \right)}{\%3}
 \end{aligned}
 \tag{89}$$

The use of the proposed risk determination expression is not meant to be an empirical metric for risk adjudication, as such an expression would need to account for many other factors that have been omitted from the scope of this content analysis study, however, is instead presented as a supporting metric for such a determination. The following plot illustrates the risk determination concept with different risk tolerances (attitudes) as areas bounded by risk curves using preset impacts.

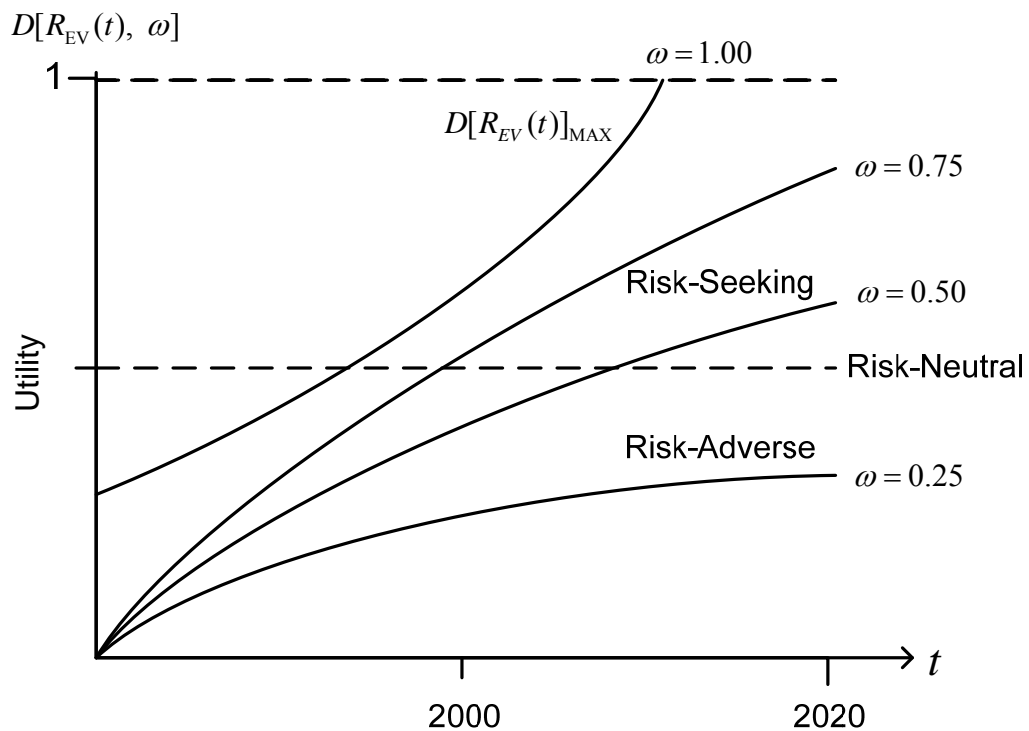


Figure 37. Risk Determination Tolerances

Another quantitative SRA approach toward risk determination would be to focus on the probability and impact of damage, for individual risks, as the probability of occurrence is time-dependent. The following figure illustrates the concept, with risk areas defined as risk adverse / normal (A1), risk-neutral / intermediate (A2), and risk-seeking / intolerable (A3) areas.

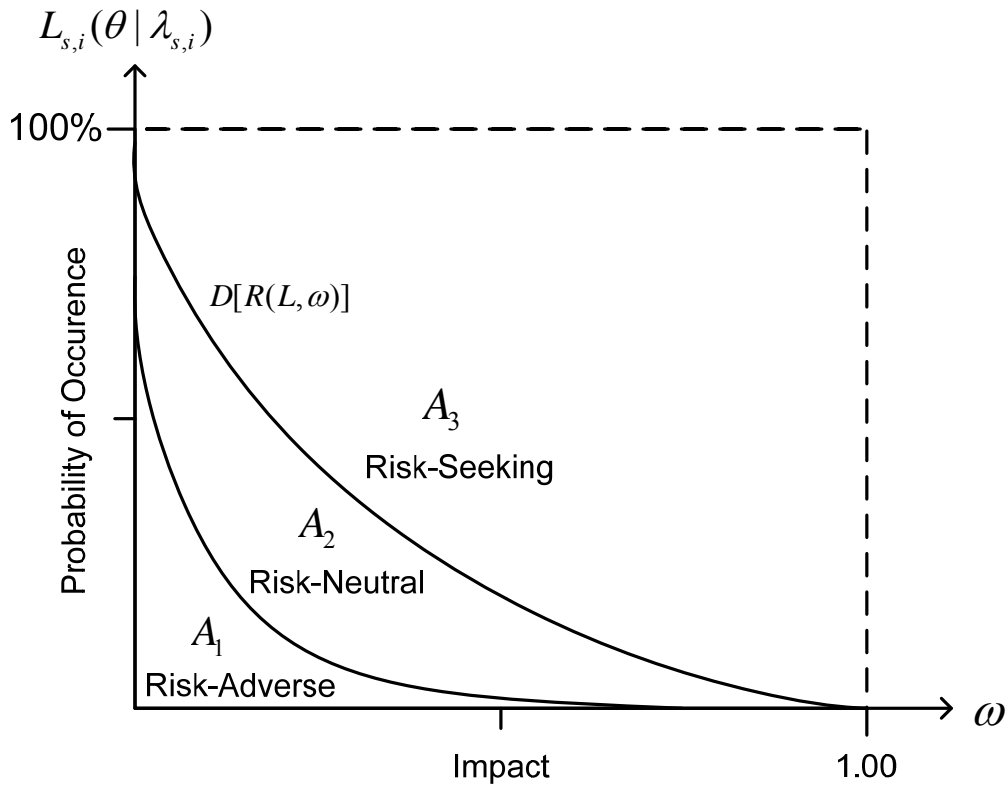


Figure 38. Risk Areas as a function of Probability and Impact

Chapter Summary

This chapter started off with an reexamination of an unique unit of measurement for risk and analyzing the application of Information Security Services (ISS): Confidentiality, Integrity, and Availability (CIA) as a risk dimension. Furthermore, a concept of risk loss confidence, in relation to expected risk, was developed in (63). An analysis of uncertainty, as it pertains to the SRA of risk, revealed an approach derived from Bayes' Theorem to practically apply likelihood figures gathered from research data. Axioms for calculating further likelihood values were also derived, and used to create probability-impact tree diagrams, for each of the risk dimensions, in providing perspective for the analysis of RQ1, and of the quantitative approach in general. The reliability of analysis, as well as, the data used for this paper were discussed, with the primary sources of data coming from US-CERT

databases and NIST NISSC surveys.

The analysis of the probability and likelihood methods toward a quantitative SRA approach for CIS yielded a modified risk expression from (43) to the expression seen in (79). It was shown from the SRA, and from RQ1, that in fact, it is possible to create a meaningful continuous, time-dependent, quantitative risk expression for CIS given existing security risk analysis (SRA) techniques. The behavior and interpretation of (79) was validated through both the analysis of its risk components and from a comparison between qualitative and quantitative risk totals. Throughout this analysis, risk components, such as the vulnerability and threat expressions, had to be modified in maintaining the mechanics of a meaningful expression. In validating the behavior of the final quantitative risk expression, a truth table was developed, showing each individual input risk component along with its corresponding output behavior, providing consistency with the full interpretation of its results. As indicated, the second part of the validation extracted special cases of CIS Test Models, developed within the methodology section, to reveal similar resulting behavior between the appraisal values of qualitative IAS totals and quantitative ISS totals.

From the SRA, and RQ2, it was shown that it is theoretically possible to create a meaningful, continuous, time-dependent, quantitative risk determination metric for CIS from a risk expression, specifically from (88) - a modification from the original risk expression in (79). A determination metric was generally expressed in (84), detailed in (89), and illustrated in Figures 36 and 37 using risk components defined from this paper. The practical application of a risk determination metric for CIS, along with its formal validity, would entail a scope suitable for a follow-on paper on the subject of SRA-CIS. The following, concluding chapter, revisits the results and elaborates on the significance of the general findings from this paper.

CHAPTER 5

CONCLUSION

Purpose of the Chapter

This chapter provides concluding statements and elaboration on the significance of this paper's general findings. The summarized findings (F1 – F10) re-emphasizes the objectives accomplished, specifically as in the formal analysis of RQ1 and RQ2, (i) providing the validation and meaningful interpretation of a proposed quantitative, time-dependent risk expression for the SRA of CIS and, (ii) a corresponding quantitative, time-dependent, risk determination metric for the operations of CIS by which an information systems authorizing official can employ.

Chapter Organization

This chapter is organized into four primary sections with the first section including a restatement of the major findings, relationships, and interpretations from the SRA of this content research. Second, further considerations about the applicability of SRA for CIS is discussed, pointing to a need to incorporate such an approach to existing RMF's. For the third section, recommendations are made for the practical application of the results this paper has produced. Additional recommendations and considerations are made in the fourth section regarding future research concerning SRA-CIS. Finally, the fourth section, of this chapter concludes this paper with advice to its reader.

Findings

To fully recap, the findings of this paper pulled apart existing qualitative considerations related to the idea of risk and then presented ways of quantitatively defining risk. Beginning with (5) through (22), the fundamental definitions of risk were taken and generalized as having the following functional construct for CIS:

$$\text{–opportunity(uncertainty)} = f[\text{impact(CONF, INT, AVAIL), probability}] \quad (\text{F1})$$

with the set of risk elements represented and identified as threats, vulnerabilities, controls, impact, and confidence:

$$\Omega = \{\theta, \lambda, \delta, \omega, \gamma\} \quad (\text{F2})$$

It was determined, that the concept of assigning probabilities to uncertainties related to risks is not new, however, the common misconception and difficulty in that the conditional probability

$$P(\lambda|\theta) \neq P(\lambda) \cdot P(\theta) \quad (\text{F3})$$

was essentially the basis for this content analysis study; driving the need for the formal analysis of RQ1 and RQ2. In light of the following definitions, both the use of Bayes' Theorem

$$P^* \propto \frac{P(\lambda)}{P(\theta)} \cdot L(\theta|\lambda) \quad (\text{F4})$$

from (49) to (52), and the probabilistic distribution modeling, of reliable vulnerability and threat database sources, (47) and (48), were conducted to practically apply likelihood values in the analysis and validation of RQ1.

The risk indices, Confidentiality, Integrity, and Availability ISS were selected as risk

dimensions for measurement, and although, a single number is not a big enough concept to communicate risk, the averaging of ISS results, using (66) and (67):

$$\text{Total Risk Appraisal} = \frac{1}{3}(\text{CONF} + \text{INT} + \text{AVAIL}) \quad (\text{F5})$$

toward consolidation into a single number, is an approach that uses caution, understanding that it involves a great loss of information.

The analysis of RQ1 found that it is possible to create a meaningful continuous, time-dependent, quantitative risk expression for CIS, given existing security risk analysis (SRA) techniques, as expressed by this author as:

$$R(t) = \int_{t_1}^{t_2} \left\{ 1 - \left[\left[P(\lambda) \cdot \frac{2}{\pi} \cdot \arctan \left(2\pi \cdot \frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t)+1]} \right) \cdot e^{-\lambda(t)} \right] \cdot [1 - \delta(t)] \right] \cdot \{\omega \cdot [1 - \gamma(\delta, t)]\} \right\} dt \quad (\text{F6})$$

based primarily on the meaningful design constraint that the product of risks approach zero:

$$\lim_{N \rightarrow \infty} \prod_i^N R_i(t) \approx 0 \quad (\text{F7})$$

and with its application validated against selected sample test case models yielding consistent behavior. The development of quantitative methods for the SRA of CIS were conducted objectively, applied to concepts of decision making involving risk, with the idea that

$$\text{Risk Rate} = \frac{d}{dt} R(t) \quad (\text{F9})$$

The analysis of RQ2 found that it is possible to create a meaningful, continuous, time-dependent, quantitative risk determination metric for CIS, as from the risk expression in RQ1.

$$\text{Risk Determination} = R \cdot R' \cdot R'' \quad (\text{F10})$$

As it was found, a risk determination metric needs to account for a ‘rate of risk’ concept. It is

illustrated in (37) and (38), that the viability of a risk determination expression, bounded by risk tolerance levels, during a Δt interval, is evaluated based on a comparison of its rate of risk with impact thresholds and likelihood figures, suggesting the nature of the risk.

Finally, it is emphasized that these findings, the purpose of SRA and risk quantification, is always to provide input to an underlying decision problem, involving not just risks, but other information security service domains, such as costs and system merit.

Conclusions

With a number of intangible and unquantifiable risk elements existing, this paper has provided a cursory examination within the field of SRA: an approach based on basic mathematical methods, which yield results that can provide relevance in the aid and guidance towards improvement of CIS, in turn, strengthening an organization's overall security posture. The ideas, analysis, and interpretation presented are based on the author's findings and analysis for the accurate representation of risk and risk adjudication.

In order to effectively apply SRA methods to CIS in operation quantitatively, it has been established that, risk data must essentially aggregate results over both a large sample and long-time duration. The current approach, being adopted, is to embrace a risk management strategy that copes with risk uncertainties through the use of qualitative methods, to include components of quantitative measures such as vulnerability management, robust response strategies, and other similar resilience perspectives (Klinke, 2002). While this risk management framework complements a qualitative approach - creating an adaptive approach to surprises through precaution-based strategies, the probability of adverse events occurring, and the handling of uncertain or vulnerable situations, cumulatively resulting in large impacts,

require the attention of a quantitative SRA approach.

In conclusion, it is prudent to reiterate that while risk determinations made by information systems authorizing officials would benefit from a truly quantitative and blanket risk decision metric for CIS that, quantitative SRA results should not be the sole basis for decision making. Uncertainty is always present it should not invalidate a risk assessment (NIST SP800-12, 1995). The purpose of this content study was to explore and highlight the viability of QRA for CIS; not to dismiss qualitative methods for quantitative ones.

Recommendations

Recommendations for use of Results

The development of risk assessment methods and procedures is an essential element in ensuring adequate security of federal information systems (NIST SP 800-53, 2010). The NIST Handbook titled, "An Introduction to Computer Security" dated October, 1995) contains guidance and recommendations on performing meaningful risk assessments. The Appendix, of this book, suggests that the preparation of formal risk analyses is no longer required, and citing that "...in the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems". Furthermore, it goes on to suggest that, "rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them" (NIST SP 800-12, 1995).

The author disagrees with the risk assessment recommendation of NIST SP 800-12, as the automation of a quantitative SRA approach would be able to provide a consistent risk

measurement methodology, with low overhead, for assessing the operations of CIS; minimizing individual analyst bias. In fact, the author would recommend, and prefer to see, the results and findings (expressions, metrics, and calculations), from this study, incorporated into an automated tracking system, to provide the real-time quantitative SRA for CIS, within a CC/S/A; providing both an overall risk appraisal figure for the organization, to include recommendations on findings for individual risk adjudication, based on pre-defined risk tolerance levels for a risk determination metric.

Recommendations for Future Research

The scope of this paper allowed for an elementary analysis on a subject of great breadth and complexity, specifically, the qualitative and time-dependent quantitative SRA for CIS. Several number of approaches and improvements could be considered in a future research effort on SRA-CIS by: (i) conducting a Factor Analysis of Information Risk (FAIR), in which a taxonomy of factors that contribute to risk would be developed, in which data establishing accurate probabilities for the frequency and magnitude of risk events are achieved, through the development of an 'in-house' vulnerability and threat incident monitor, thus, obtaining statistical data, representative of the target assessment environment, for the probabilistic modeling of the expression in (24); (ii) re-evaluating the general impact factor expression in (31), for use in quantitative analysis, as it's currently based on a completely qualitative (High, Medium, Low) severity/impact category (CAT) scale, to instead adopt specific exposure/impact coefficient values unique to individual threats applicable to the CIS under analysis; (iii) accounting for all MAC levels, to include MAC II (mission essential), and MAC III (mission support) IS, with classifications which include both sensitive and public

data – note, the findings of this paper is specific to MAC I (mission critical), classified CIS; (iv) further researching of risk variables, which may additionally serve as measures of merit for information assurance, appending on CIA to include Authentication, Non-repudiation, Utility, Resilience and Visibility; (v) expanding beyond the probability of occurrence regarding the criteria range for risk evaluation and determination to include adverse effects in natural units (human life and cost), Incertitude, Ubiquity, Persistency, Reversibility, latency / delayed effect between the initial event and the actual impact of damage, and also the violation of equities or the discrepancy between benefits and risks.

Summary

In today's threat environment having an effective risk assessment methodology, within a CC/S/A's security program, is vital in protecting Critical Information Systems. In summary, there is no simple recipe for the quantification of risk. Security Risk Analysis is a heterogeneous phenomenon with its statistical nature limited by the uncertainty inherit with underlying data and within the methodology itself. The practicality and interpretation of quantifying risk for information systems remains an open problem.

Security Risk Analysis, adopting both qualitative and quantitative methodologies, can be a viable and meaningful approach in assessing, evaluating, and managing risks resulting from the operation of Critical Information Systems. Ultimately, it is the author's desire, by seeking analytics in characterizing and expressing uncertainty in risk that the content analysis from this thesis has brought upon added value and perspective to the reader's comprehension of SRA-CIS.

Appendix

List of Equations

$$ALE = SLE \times ARO \quad (1)$$

$$SLE = \text{asset value} \times EF \quad (2)$$

$$(\text{ALE without safeguard}) - (\text{ALE with safeguard}) - (\text{annual cost of safeguard}) \quad (3)$$

$$\text{countermeasure costs} < \text{potential loss} \quad (4)$$

$$\text{Risk} = -\text{Opportunity} \quad (5)$$

$$\text{Uncertainty} = 100\% - \text{confidence} \quad (6)$$

$$\text{Risk} = f_{\text{impact}}(\text{uncertainty}) \quad (7)$$

$$\text{Risk} = -|f_{\text{impact}}(100\% - \text{confidence})| = \text{loss} \quad (8)$$

$$\text{Risk} = f(\text{impact, probability}) = f[\omega_i, P(i)] \quad (9)$$

$$\text{Risk}_{EV} = \sum_n \omega_{i,n} \cdot P(i) \quad (10)$$

$$\text{Risk} = f[\text{impact, probability}(\text{vulnerability} | \text{threat})] \quad (11)$$

$$= f[\omega_i, P_i(\lambda_i | \theta_i)] \quad (12)$$

$$\text{Risk}_{EV} = \sum_n \omega_{i,n} \cdot P_i(\lambda_i | \theta_i) \quad (13)$$

$$\neq \sum_n \omega_{i,n} \cdot P_i(\lambda_i) \cdot P_i(\theta_i) \quad (14)$$

$$0 \leq P_i(\lambda_i | \theta_i) \leq 1 \quad (15)$$

$$0 \leq P_i(\lambda_i) \leq P_i(\theta_i) \leq 1 \quad (16)$$

$$\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact} \quad (17)$$

$$E_i = [D_i, P_i] \quad (18)$$

$$U = \sum_{i=1}^n (E_i + \bar{E}_i) = \sum_{i=1}^n \{ [D_i, P_i] + [\bar{D}_i, (1 - P_i)] \} \quad (19)$$

$$\text{Information Security} = \text{CONF} + \text{INT} + \text{AVAIL} \quad (20)$$

$$\text{Risk} = f \left[\text{impact}(\text{CIA Services, CAT Rating, MAC, costs}), \text{probability} \right] \quad (21)$$

$$= f \left[\omega_i(\text{CONF, INT, AVAIL}, \omega_{\text{CAT}}), P_i(\lambda_i | \theta_i) \right] \quad (22)$$

$$\omega_{s,n} \cdot (1 - \gamma_{s,n}) \quad (23)$$

$$P_{s,i}(\lambda_{s,i} | \theta_{s,i}) = \frac{P(\lambda_{s,i} \cap \theta_{s,i})}{P(\lambda_{s,i})} = \frac{n(\lambda_{s,i} \cdot \theta_{s,i})}{n(\theta_{s,i})} \quad (24)$$

$$1 - \delta_{s,i} \quad (25)$$

$$\delta_{s,i} = \begin{cases} 0, & \text{iff Non-Compliant (NC)} \\ 1, & \text{if Compliant (C) } \oplus \text{ Not Applicable (N/A)} \end{cases} \quad (26)$$

$$P_{s,i}(\lambda_{s,i} | \theta_{s,i}) \cdot (1 - \delta_{s,i}) \quad (27)$$

$$\text{Risk}_{\text{EV}} = \prod_i^N R_i \quad (28)$$

$$\lim_{N \rightarrow \infty} \text{Risk}_{\text{EV}} \simeq 0 \quad (29)$$

$$\text{Risk} \neq 0 \quad (30)$$

$$\omega_{s,i} = \frac{1}{100} \left(1 - \left| -12.5\omega_{\text{CAT}}^2 + 67.5\omega_{\text{CAT}} - 95 \right| \right) \quad (31)$$

$$\text{Risk}_i(\Omega) = \neg\gamma \wedge \omega \wedge U \quad (32)$$

$$= \neg\gamma \wedge \omega \wedge (\neg E \vee E) \quad (33)$$

$$\text{Risk}_i(\Omega) = \neg\gamma \wedge \omega \wedge E \quad (34)$$

$$= \neg\gamma \wedge \omega \wedge (D \wedge P_i) \quad (35)$$

$$= \neg\gamma \wedge \omega \wedge [\neg\delta \wedge (\text{CONF} \vee \text{INT} \vee \text{AVAIL}) \wedge (\theta \wedge \lambda)] \wedge (\theta \wedge \lambda) \quad (36)$$

$$= \neg\gamma \wedge \omega \wedge [\neg\delta \wedge (\text{CONF} \vee \text{INT} \vee \text{AVAIL}) \wedge \theta \wedge \lambda] \quad (37)$$

$$= \theta \wedge \lambda \wedge \neg\delta \wedge \omega \wedge \neg\gamma \wedge (\text{CONF} \vee \text{INT} \vee \text{AVAIL}) \quad (38)$$

$$\Omega_i = \{ \langle \theta_i, \lambda_i, \delta_i, \omega_i, \gamma_i, U \rangle \} \quad (39)$$

$$\text{Risk}_{\text{EV}}(\Omega_i) = \prod_{n=1}^A \sum_{s=1}^B \sum_{i=1}^{C(s)} \{ 1 - [\text{P}_{s,i}(\lambda_{s,i} | \theta_{s,i}) \cdot (1 - \delta_{s,i})] \cdot [(\omega_{s,n}) \cdot (1 - \gamma_{s,n})] \} \quad (40)$$

$$A = \begin{cases} 1, \text{ Confidence (CONF)} \\ 2, \text{ Integrity (INT)} \\ 3, \text{ Availability (AVAIL)} \end{cases} \quad B = \begin{cases} 1, \text{ Physical Security} \\ 2, \text{ Cyber Security} \\ 3, \text{ Continuity} \\ 4, \text{ Security Design} \\ 5, \text{ Security Education} \\ 6, \text{ Identity A\&A} \\ 7, \text{ Content Security} \end{cases} \quad C(s) = \begin{cases} 23 \text{ iff } s = 1, \\ 35 \text{ iff } s = 2, \\ 17 \text{ iff } s = 3, \\ 39 \text{ iff } s = 4, \\ 6 \text{ iff } s = 5, \\ 18 \text{ iff } s = 6, \\ 4 \text{ iff } s = 7 \end{cases} \quad (41)$$

$$R_n(t) = \int_U \{ 1 - \{ \text{P}[\lambda(t) | \theta(t)] \cdot [1 - \delta(t)] \} \cdot \{ \omega \cdot [1 - \gamma(\delta, t)] \} \} dt \quad (42)$$

$$= dt \Big|_U - \int_U \omega \cdot \text{P}[\lambda(t) | \theta(t)] \cdot [1 - \delta(t)] \cdot [1 - \gamma(\delta, t)] dt \quad (43)$$

$$\text{Risk Determination} = \text{Risk} \times \text{Risk Rate} \times \text{Risk Rate Variance} \quad (44)$$

$$D(R) = R \cdot R' \cdot R'' \quad (45)$$

$$D^*(R) = R \cdot \left[1 + \frac{2}{\pi} \tan^{-1} \left(\frac{dR}{dt} \right) \right] \left[1 + \frac{2}{\pi} \tan^{-1} \left(\frac{d^2R}{dt^2} \right) \right] \quad (46)$$

$$\lambda(t) = (73)t^2 - (2.9 \cdot 10^5)t + (2.9 \cdot 10^8) \quad (47)$$

$$\theta(t) = (4.5 \cdot 10^3)t^2 - (1.8 \cdot 10^7)t + (1.8 \cdot 10^{10}) \quad (48)$$

$$P^* = P_{n,s}(\lambda | \theta) \tag{49}$$

$$= \frac{P(\lambda) \cdot L(\theta_{n,s}, \dots, \theta_{n,7} | \lambda_{s,i})}{P(\theta)} \tag{50}$$

$$\propto P(\lambda) \cdot L(\theta_{n,s} | \lambda_{s,i}) \tag{51}$$

$$\lim_{t \rightarrow \infty} P_{n,s}[\theta(t)] = 1 \tag{52}$$

$$C_{TOTAL} = 2 \times_{n\{P\}} \left[\sum_{r=1}^3 \binom{3}{r} \right]_{n\{A,B,C\}} \cdot \left[\sum_{r=1}^3 \binom{3}{r} \right]_{n\{I,J,K\}} \cdot \left[\sum_{r=1}^7 \binom{7}{r} - 23 \right]_{n\{Q,R,S,T,U,V,W\}} + \frac{1}{n\{Y\}} \tag{53}$$

$$C_{TOTAL} = 2 \times [{}_3C_3 + {}_3C_2 + {}_3C_1] \cdot [{}_3C_3 + {}_3C_2 + {}_3C_1] \cdot [{}_7C_7 + {}_7C_6 + {}_7C_5 + {}_7C_4 + {}_7C_3 + \dots \\ \dots + {}_7C_2 + {}_7C_1 - 23] + 1 \tag{54}$$

$$C_{TOTAL} = 11,939 \tag{55}$$

$$s = \frac{s_0}{\left(1 + \frac{s_0 - 1}{C_{TOTAL}} \right)} \tag{56}$$

$$s \approx 100 \tag{57}$$

$$s_0 = \frac{Z^2 p(1-p)}{e^2} \tag{58}$$

$$Z = +1\sigma \tag{59}$$

$$p = 0.50 \tag{60}$$

$$e = 0.05 \quad (61)$$

$$\text{Risk}_{\text{EV}} = 100\% - (\text{Risk Loss Confidence}) \quad (62)$$

$$R_{\text{LC}} = 1 - R_{\text{EV}} \quad (63)$$

$$0\% \leq \text{Risk Loss Confidence} < 100\% \quad (64)$$

$$R_{\text{LC}} \neq 1 \quad (65)$$

$$\text{Total Information Security Risk Appraisal} = \frac{1}{N} \sum_{n=1}^N (\text{ISS})_n \quad (66)$$

$$R_{\text{TOTAL}} = \frac{1}{3} (\text{CONF}_{n=1} + \text{INT}_{n=2} + \text{AVAIL}_{n=3}) \quad (67)$$

$$\text{Security Confidence} = \min(|\text{IAS}|_{s=1}, \dots, |\text{IAS}|_{s=7}) \quad (68)$$

$$P(\theta) \cdot P(\lambda | \theta) = P(\lambda) \cdot L(\theta | \lambda) \quad (69)$$

$$L(\theta | \lambda) = \frac{1}{P(\lambda)} \cdot P(\lambda | \theta) \quad (70)$$

$$L_{s,i}(\theta | \lambda_{s,i}) = \frac{1}{P_{s,i}(\lambda)} \cdot P_{s,i}(\lambda_{s,i} | \theta, \delta_{s,i}) \quad (71)$$

$$= k \cdot P_{s,i}(\lambda_{s,i} | \theta, \delta_{s,i} = 0) \times P_{s,i}(\lambda_{s,i} | \theta, \delta_{s,i} = 1) \times \bar{E}_i \quad (72)$$

$$L(\theta | \lambda) = k \cdot \prod_{N=1}^{n(\lambda)} P(\lambda_N | \theta, \delta) \quad (73)$$

$$L_{n,s}(\theta | \lambda_{s,i}) = \prod_{N=1}^{n(L)} L_{s,i}(\theta | \lambda_{s,i}, \delta_{s,i}) \quad (74)$$

$$L_{n,s}(\theta | \lambda_{s,i}) = w_N \cdot \sum_{N=1}^{n(L)} L_{s,i}(\theta | \lambda_{s,i}, \delta_{s,i}) \quad (75)$$

$$\sum_{N=1}^{n(L)} w_N = \frac{\omega_{s,i} + \dots + \omega_N}{\sum_N (\omega_{s,i} + \dots + \omega_N)} = 1 \quad (76)$$

$$L(\theta | \lambda) = \left(\frac{\lambda(t)^{\theta(t)}}{\theta(t)!} \right) \cdot e^{-\lambda(t)} \quad (77)$$

$$P_{n,s}(\lambda | \theta) \propto P(\lambda) \cdot \left(\frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t) + 1]} \right) \cdot e^{-\lambda(t)} \quad (78)$$

$$R_{s,i}(t) = \int_{t_1}^{t_2} \left\{ 1 - \left[P_{s,i}(\lambda) \cdot \left(\frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t) + 1]} \right) \cdot e^{-\lambda(t)} \right] \cdot [1 - \delta_{s,i}(t)] \right\} \cdot \{ \omega_{s,i} \cdot [1 - \gamma(\delta_{s,i}, t)] \} dt \quad (79)$$

$$\omega_{\text{CAT}} = \begin{cases} 1, & \text{if CAT I} \\ 2, & \text{if CAT II} \\ 3, & \text{if CAT III} \end{cases} \quad (80)$$

$$0 \leq \gamma(\delta_{s,i}, t) \leq 1 \quad (81)$$

$$P^* \propto P(\lambda) \cdot \left[\frac{(73t^2 - 2.9 \cdot 10^5 t + 2.9 \cdot 10^8)^{4500(t-2000)^2}}{\Gamma(4.5 \cdot 10^3 t^2 - 1.8 \cdot 10^7 t + 1.8 \cdot 10^7)} \right] \cdot e^{-73t^2 + 2.9 \cdot 10^5 t - 2.9 \cdot 10^8} \quad (82)$$

$$P^* \propto P(\lambda) \cdot \left[\frac{2}{\pi} \cdot \arctan \left(2\pi \cdot \frac{\left(\frac{73}{18000000} t^2 - \frac{29}{1800} t + \frac{145}{9} \right)^{1/4000(t-2000)^2}}{\Gamma\left(\frac{1}{4000} t^2 - t + 1001\right)} \right) \right] \cdot e^{\frac{-73}{18000000} t^2 + \frac{29}{1800} t - \frac{145}{9}} \quad (83)$$

$$D(R) = R_{s,i}(t) \cdot \frac{dR_{s,i}(t)}{dt} \cdot \frac{d^2R_{s,i}(t)}{dt^2} \tag{84}$$

$$R_{s,i}(t) = \int_{t_1}^{t_2} \left\{ 1 - \left[P_{s,i}(\lambda) \cdot \frac{2}{\pi} \cdot \arctan \left(2\pi \cdot \frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t)+1]} \cdot e^{-\lambda(t)} \right) \cdot [1 - \delta_{s,i}(t)] \right] \cdot \{ \omega_{s,i} \cdot [1 - \gamma(\delta_{s,i}, t)] \} \right\} dt \tag{85}$$

$$\Omega_{sc} \in \{P_{s,i}(\lambda), \omega_{s,i}, [1 - \delta_{s,i}(t)], [1 - \gamma(\delta_{s,i}, t)]\} \tag{86}$$

$$\Omega_{sc} = 1 \tag{87}$$

$$R_{s,i}(t) = \int_{t_1}^{t_2} \left(\frac{\lambda(t)^{\theta(t)}}{\Gamma[\theta(t)+1]} \cdot e^{-\lambda(t)} \right) dt \tag{88}$$

Refer to Page 88 (89)

Refer to Pages 93 & 94 (F1-F10)

References

- Abdi, H. (2003). Multivariate analysis. In M. Lewis-Beck, A. Bryman, & T. Futing (Eds): Encyclopedia for research methods for the social sciences. Thousand Oaks (CA): Sage.
Retrieved July 23, 2011 from
http://www.google.com/url?sa=t&source=web&cd=3&ved=0CDYQFjAC&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.13.6446%26rep%3Drep1%26type%3Dpdf&rct=j&q=multivariate%20analysis&ei=hJorTo6eEIrRiAKWnKWwAg&usg=AFQjCNEQpclZOGZJtU1CjJPMqxSt_aboBw
- AIRMIC. (2002). A risk management standard. Retrieved July 14, 2011 from
http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf
- Almer, B. (1965). Modern general risk theory. Astin Volume 4, No. 2. Retrieved July 14, 2011 from
<http://www.casact.org/library/astin/vol4no2/136.pdf>
- Apostolakis, G. (2004). How useful is quantitative risk analysis? Risk Analysis, Vol. 24, No. 3. Retrieved July 24, 2011 from
<http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/7.pdf>
- Bartha, P. (2000). Phil 460: Week 3 The probability Calculus. Retrieved July 23, 2011 from
<http://faculty.arts.ubc.ca/pbartha/p460f08/probho.pdf>
- Bell, S. (1999, August). Bell, S. (1999, August). Measurement good practice guide no.11 (issue 2) a beginner's guide to uncertainty of measurement. Center for basic, thermal and length metrology national physical lab. Retrieved September 16, 2011 from
http://www.wmo.int/pages/prog/gcos/documents/gruanmanuals/UK_NPL/mgpg11.pdf

- Birch, D., McEvoy, N. (1992). Risk analysis for information systems. *Journal of Information Technology* 7, 44-53. Surrey, UK. Retrieved July 14, 2011 from <http://paul-hadrien.info/backup/LSE/IS%20490/risk%20analysis%20and%20IS.pdf>
- Buckshaw, D. (2005). Mission oriented risk and design analysis of critical information systems. *Military Operations Research*, V10 N2. Retrieved July 14, 2011 from <http://www.innovatedecisions.com/documents/Buckshaw-Parnell.pdf>
- Buhlmann, H. (2005). *Mathematical methods in risk theory*. Springer-Verlag Berlin Heidelberg, New York.
- CDW-G. (2011). Risk assessment and data loss prevention. Retrieved August 30, 2011 from <http://www.edtechmag.com/higher/images/2011/updates/88890-wp-risk%20assessment%20df.pdf>
- CERT.org. (2006, September). CSO magazine 2006 e-crime watch survey. Retrieved November 3, 2011 from <http://www.cert.org/archieve/pdf/ecrimesurvey06.pdf>
- Chief Information Officer Policy and Guidance Memorandum #20. (2008, July). USPACOM security certification and accreditation policy and guidance. United States Pacific Command.
- Cieslak, R. (2009, April). U.S. Pacific Command chief information officer guidance: Information assurance framework. United States Pacific Command.
- Cieslak, R., Fink, M. (2011, May). U.S. Pacific Command Information services references model (ISRM) Version 1.7. United States Pacific Command.
- CJCSI 6510.01F. (2011, February). Information assurance and computer network defense. Retrieved June 27, 2011 from http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

- Clemen, R., Winkler, R. (1997, October). Combining probability distributions from experts in risk analysis. Duke University, NC. Retrieved July 14, 2011 from http://www.cob.ohio-state.edu/~butler_267/DAPapers/WP970009.pdf
- CMMI-DEV. (2010, November). Capability maturity model and CMM integration. Retrieved June 27, 2011 from http://www.sei.cmu.edu/cmml/tools/cmmiv1-3/upload/CMMI-DEV_Quick_Ref.pdf
- CNSSD-500. (2006, August). Information assurance education, training, and awareness. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/CNSSD_500.pdf
- CNSSD-502. (2004, December). National directive on security of national security systems. Retrieved June 27, 2011 from <http://www.cnss.gov/Assets/pdf/CNSSD-502.pdf>
- CNSSI-1253. (2009, October). Security categorization and control selection for national security systems. Retrieved June 27, 2011 from <http://www.cnss.gov/Assets/pdf/CNSSI-1253.pdf>
- CNSSI-4009. (2010, April). National information systems security glossary. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
- CNSSI-4012. (2004, June). National information assurance training standard for senior systems managers. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/cnssi_4012.pdf
- CNSSI-4013. (2004, March). National information assurance training standard for senior systems administrators. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/cnssi_4013.pdf

CNSSI-4014. (2004, April). Information assurance training standard for information systems security officers. Retrieved June 27, 2011 from

http://www.cnss.gov/Assets/pdf/cnssi_4014.pdf

CNSSI-4016. (2005, November). National information assurance training standard for risk analysts. Retrieved June 27, 2011 from <http://www.cnss.gov/Assets/pdf/cnssi-4016.pdf>

CNSSP-6. (2005, October). National policy on certification and accreditation of national security telecommunications and information systems. Retrieved June 27, 2011 from

<http://www.cnss.gov/Assets/pdf/CNSSP-6.PDF>

CNSSP-14. (2002, November). National policy governing the release of information assurance products and services that are not a part of the federal government. Retrieved June 27,

2011 from http://www.cnss.gov/Assets/pdf/CNSSP_14.PDF

CNSSP-22. (2009, February). Information assurance risk management policy for national security systems. Retrieved June 27, 2011 from [http://www.cnss.gov/Assets/pdf/CNSSP-](http://www.cnss.gov/Assets/pdf/CNSSP-22.pdf)

[22.pdf](http://www.cnss.gov/Assets/pdf/CNSSP-22.pdf)

CNSSP-24. (2010, May). Policy on assured information sharing for national security systems.

Retrieved June 27, 2011 from <http://www.cnss.gov/Assets/pdf/CNSSP-24.pdf>

Common Criteria. (2009, June). Common criteria for information technology security

evaluation. Retrieved June 27, 2011 from

[http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3%20-](http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3%20-%20marked%20changes.pdf)

[%20marked%20changes.pdf](http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3%20-%20marked%20changes.pdf)

- Cumings, M., McGarvey, D., Vinch, P. (2006, June). Homeland security risk assessment volume II methods, techniques, and tools. Retrieved July 31, 2011 from <http://www.homelandsecurity.org/hsireports/Risk%20Assessment%20Volume%202%20Methods%20Techniques%20and%20Tools.pdf>
- Devost, M. (2008). Systems security engineering capability maturity model. Retrieved July 23, 2011 from <http://www.devost.net/papers/business-briefing.pdf>
- DoD 5220.22-M. (2006, February). National industrial security program operating manual. Retrieved June 27, 2011 from <http://www.dss.mil/isp/odaa/documents/nispom2006-5220.pdf>
- DoD 8320.2-G. (2006, April). Guidance for implementing net-centric data sharing. Retrieved June 27, 2011 from <http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf>
- DoD 8570.01-M. (2010, April). Information assurance workforce improvement program. Retrieved June 27, 2011 from <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>
- DoD PMBOK. (2003, June). U.S. DoD extension to: a guide to the project management body of knowledge. Retrieved June 27, 2011 from <http://www.dau.mil/pubs/gdbks/DoDExtPMBOK--June%2003.pdf>
- DoDAF. (2009, May). The DoDAF architecture framework version 2.0. Retrieved June 27, 2011 from http://cio-nii.defense.gov/sites/dodaf20/products/DoDAF_2-0_web.pdf
- DoDD 5144.1. (2005, May). Assistant secretary of defense for networks and information integration/DoD chief information officer. Retrieved June 27, 2011 from <http://www.dtic.mil/whs/directives/corres/pdf/514401p.pdf>
- DoDD 8100.1. (2003, November). Global information grid overarching policy. Retrieved June 27, 2011 from <http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf>

DoDD 8100.02. (2004, April). Use of commercial wireless devices, services and technologies in the department of defense global information grid. Retrieved June 27, 2011 from

<http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf>

DoDD 8500.01E. (2007, April). Information assurance. Retrieved June 27, 2011 from

<http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>

DoDD 8500-2-MACI-CLASS. (2008, March). IA control checklist – MAC 1 - Classified.

Retrieved June 27, 2011 from [http://diacapservices.com/files/DoDI_8500-](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_1-Classified_-_28_March_2008.37111529.pdf)

[2_IA_Control_Checklist_-_MAC_1-Classified_-_28_March_2008.37111529.pdf](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_1-Classified_-_28_March_2008.37111529.pdf)

DoDD 8500-2-MACI-P. (2008, March). IA control checklist – MAC 1 - Public. Retrieved

June 27, 2011 from [http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_1-Public_-_28_March_2008.305113323.pdf)

[MAC_1-Public_-_28_March_2008.305113323.pdf](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_1-Public_-_28_March_2008.305113323.pdf)

DoDD 8500-2-MACI-SEN. (2008, March). IA control checklist – MAC 1 - Sensitive.

Retrieved June 27, 2011 from [http://diacapservices.com/files/DoDI_8500-](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_1-Sensitive_-_28_March_2008.305113121.pdf)

[2_IA_Control_Checklist_-_MAC_1-Sensitive_-_28_March_2008.305113121.pdf](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_1-Sensitive_-_28_March_2008.305113121.pdf)

DoDD 8500-2-MACII-CLASS. (2008, March). IA control checklist – MAC 2 - Classified.

Retrieved June 27, 2011 from [http://diacapservices.com/files/DoDI_8500-](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_2-Classified_-_28_March_2008.305112844.pdf)

[2_IA_Control_Checklist_-_MAC_2-Classified_-_28_March_2008.305112844.pdf](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_2-Classified_-_28_March_2008.305112844.pdf)

DoDD 8500-2-MACII-P. (2008, March). IA control checklist – MAC 2 - Public. Retrieved

June 27, 2011 from [http://diacapservices.com/files/DoDI_8500-](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_2-Public_-_28_March_2008.305114045.pdf)

[2_IA_Control_Checklist_-_MAC_2-Public_-_28_March_2008.305114045.pdf](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_2-Public_-_28_March_2008.305114045.pdf)

DoDD 8500-2-MACII-SEN. (2008, March). IA control checklist – MAC 2 - Sensitive.

Retrieved June 27, 2011 from [http://diacapservices.com/files/DoDI_8500-](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_2-Sensitive_-_28_March_2008.305113850.pdf)

[2_IA_Control_Checklist_-_MAC_2-Sensitive_-_28_March_2008.305113850.pdf](http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_2-Sensitive_-_28_March_2008.305113850.pdf)

DoDD 8500-3-MACIII-CLASS. (2008, March). IA control checklist – MAC 3 - Classified.

Retrieved June 27, 2011 from http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_3-Classified_-_28_March_2008.305114254.pdf

DoDD 8500-3-MACIII-P. (2008, March). IA control checklist – MAC 3 - Public. Retrieved

June 27, 2011 from http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_3-Public_-_28_March_2008.305114653.pdf

DoDD 8500-3-MACIII-SEN. (2008, March). IA control checklist – MAC 3 - Sensitive.

Retrieved June 27, 2011 from http://diacapservices.com/files/DoDI_8500-2_IA_Control_Checklist_-_MAC_3-Sensitive_-_28_March_2008.305114455.pdf

DoDI 8500.2. (2003, February). Information assurance implementation. Retrieved June 27,

2011 from <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>

DoDI 8510.01. (2007, November). DoD information assurance certification and accreditation process. Retrieved October 18, 2011 from

<http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>

DoDI 8551.1. (2004, August). Ports, protocols, and services management. Retrieved June 27,

2011 from <http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf>

Elky, S. (2006). An introduction to information system risk management. Retrieved August

30, 2011 from http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204

Endsley, M., Jones, W. (1997, February). Situation awareness information dominance & information warfare. *United States Air Force Armstrong Laboratory*. AL/CF-TR-1997-0156. Retrieved July 10, 2011 from

<http://www.satechnologies.com/Papers/pdf/IW%26SAreport%20.pdf>

- FIPS PUB 199 (2004, February). Standards for security categorization of federal information and information systems. Retrieved August 11, 2011 from <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- GAO/AMID-99-139. (1999, August). Information security risk assessment practices of leading organizations. Retrieved July 10, 2011 from <http://dodreports.com/pdf/ada391082.pdf>
- Gibson, M. (1997, March). Information systems for risk management. Federal Reserve Board. Retrieved July 10, 2011 from <http://www.bis.org/publ/ecsc07f.pdf>
- Haasl, D. (1965, June). Advanced concepts in fault tree analysis. Retrieved July 31, 2011 from <http://www.fault-tree.net/papers/haasl-advanced-concepts-in-fta.pdf>
- Haimes, Y., Li, D., Tulsiani, V. (1990). Multiobjective decision-tree analysis. Risk Analysis, Vol. 10, No. 1. Retrieved July 24, 2011 from <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/20.pdf>
- Hansche, S. (2005). Official guide to the cissp-issep cbk. Second Edition, ISC2.
- Harris, S. (2008). CISSP all in one exam guide, fourth edition. McGraw-Hill, New York, NY.
- Heemstra, F., Kusters, R., Nijhuis, R. (1997). Dealing with risk: beyond gut feeling: an approach to risk management in software engineering. Retrieved September 12, 2011 from <http://alexandria.tue.nl/repository/books/493355.pdf>
- IEEE Std 1220-2005. (2005, September). IEEE standard for application and management of the systems engineering process. *IEEE*. New York, NY. Retrieved June 27, 2011 from http://tolerancezero.net/files/index.php?dir=asgp08%2Fcontendos%2FReferencias%2F&download=ISO_IEC+26702+IEEE+Std+1220-2005.pdf

ISO 31000. (2008). Risk management – Principles and guidelines on implementation.

Retrieved August 11, 2011 from http://ddata.over-blog.com/xxxyyy/0/32/13/25/Risques/ISO_DIS_31000_-E--1-.pdf

ISSDD. (2010, January). *Information system service description document*. United States Pacific Command.

Jedamus, P., Frame, R. (1969). *Business decision theory*. McGraw-Hill Book Company.

Johnson, D. (2005, May). Best practices in information assurance and information technology networking in organizations that have two departments. Retrieved August 30, 2011 from <http://ac-support.europe.umuc.edu/~meinkej/inss690/johnson.pdf>

Jones, J. (2008). Risk evolution. Retrieved August 25, 2011 from http://www.riskmanagementinsight.com/media/documents/Risk_Evolution.pdf

Jorion, P. (2006). The new benchmark for managing financial risk. Retrieved September 2, 2011 from <http://merage.uci.edu/~jorion/Answer.pdf>

Kaplan, S., Garrick, B. (1981). On the quantitative definition of risk. *Risk Analysis*, Vol. 1, No. 1. Retrieved July 24, 2011 from <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/3.pdf>

Kastenber, W., Leslie, C. (1985). Value/impact assessment for the evaluation of risk reduction: Development of a framework. *Reliability Engineering and System Safety*, Vol. 28, pp. 205-227. Retrieved July 24, 2011 from <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/19.pdf>

Kastenber, W., Solomon, K. (1985). On the use of confidence levels in risk management. *Journal of Hazardous Materials*, Vol. 10, pp. 263-278. Retrieved July 24, 2011 from <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/16.pdf>

- Kinamik. (2007). The CIA triad: have you thought about integrity?. Retrieved September 3, 2011 from http://www.kinamik.com/download/Kinamik-Whitepaper_CIA.pdf
- Klinke, A., Ortwin, R. (2002). A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies. *Risk Analysis*, Vol. 22, No. 6. Retrieved July 24, 2011 from <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/6.pdf>
- Kyburg, H. (1970). Probability and inductive logic, chapter 6: subjectivistic interpretations of probability. Retrieved September 12, 2011 from http://fitelson.org/probability/kyburg_6.pdf
- Mauw, S., Oostdijk, M. (2005, November). Foundations of attack trees. Retrieved July 31, 2011 from <http://www.win.tue.nl/~sjouke/publications/papers/attacktrees.pdf>
- McAfee Labs. (2011). McAfee threats report: First quarter 2011. Retrieved July 23, 2011 from <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2011.pdf>
- Meritt, J. (1999). A method for quantitative risk analysis. Retrieved June 27, 2011 from <http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf>
- Morgan, M., Florig, H., Dekay, M. (2000). Categorizing risks for risk ranking. *Risk Analysis*, Vol. 20, No. 1. Retrieved July 23, 2011 from <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/5.pdf>
- Multivariate Analysis. (2007). Chapter 1 concepts. Retrieved July 23, 2011 from <http://support.sas.com/publishing/pubcat/chaps/56903.pdf>
- NIST SP 800-12. (1995, October). An introduction to computer security: The NIST handbook. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

NIST SP 800-14. (1996, September). Generally accepted principles and practices for securing information technology systems. *NIST Publications, Computer Security Division*.

Gaithersburg, MD. Retrieved June 27, 2011 from

<http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>

NIST SP 800-18. (2006, February). Guide for developing security plans for information technology systems. *NIST Publications, Computer Security Division*. Gaithersburg, MD.

Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-18->

[Rev1/sp800-18-Rev1-final.pdf](http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf)

NIST SP 800-23. (2000, August). Guideline to federal organizations on security assurance and acquisition/use of tested/evaluated products. *NIST Publications, Computer Security*

Division. Gaithersburg, MD. Retrieved June 27, 2011 from

<http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf>

NIST SP 800-25. (2000, October). Federal agency use of public key technology for digital signatures and authentication. *NIST Publications, Computer Security Division*.

Gaithersburg, MD. Retrieved June 27, 2011 from

<http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf>

NIST SP 800-27. (2004, June). Engineering principles for information technology security (a baseline for achieving security). *NIST Publications, Computer Security Division*.

Gaithersburg, MD. Retrieved June 27, 2011 from

<http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>

NIST SP 800-30. (2002, July). Risk management guide for information technology systems.

NIST Publications, Computer Security Division. Gaithersburg, MD. Retrieved June 27,

2011 from <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

NIST SP 800-34. (2010, May). Contingency planning guide for federal information systems.

NIST Publications, Computer Security Division. Gaithersburg, MD. Retrieved June 27, 2011 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NIST SP 800-35. (2003, October). Guide to information technology security services. *NIST*

Publications, Computer Security Division. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf>

NIST SP 800-36. (2003, October). Guide to selecting information technology security

products. *NIST Publications, Computer Security Division.* Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>

NIST SP 800-37. (2010, February). Guide to applying the risk management framework to

federal information systems: a security life cycle approach. *NIST Publications, Computer Security Division.* Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

NIST SP 800-39. (2011, March). Managing information security risk. *NIST Publications,*

Computer Security Division. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

NIST SP 800-47. (2002, August). Security guide for interconnecting information technology

systems. *NIST Publications, Computer Security Division.* Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf>

- NIST SP 800-53. (2010, May). Recommended security controls for federal information systems and organizations. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- NIST SP 800-55. (2008, July). Performance measurement guide for information security. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>
- NIST SP 800-59. (2003, August). Guideline for identifying an information system as a national security system. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf>
- NIST SP 800-60. (2008, August). Guide for mapping types of information and information systems to security categories. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
- NIST SP 800-64. (2008, October). Security considerations in the information system development life cycle. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>
- NIST SP 800-65. (2005, January). Integrating IT security into the capital planning and investment control process. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/drafts/800-65-rev1/draft-sp800-65rev1.pdf>

NIST SP 800-100. (2006, October). Information security handbook: a guide for managers.

NIST Publications, Computer Security Division. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>

NIST SP 800-115. (2008, September). Technical guide to information security testing. *NIST*

Publications, Computer Security Division. Gaithersburg, MD. Retrieved June 27, 2011 from <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

Novosyolov, A. (2003). Characteristic classes of families of risk measures. Institute of

Computational Modeling, Krasnoyarsk, Russia. Retrieved June 27, 2011 from http://risktheory.net/papers/fam2003_2e.pdf

Novosyolov, A. (2003). Combined functionals as risk measures. Institute of Computational

Modeling, Krasnoyarsk, Russia. Retrieved June 27, 2011 from <http://risktheory.net/papers/bowles2003.pdf>

Novosyolov, A. (2003). Inverse problems of risk theory and characteristic classes of

distributions. Institute of Computational Modeling, Krasnoyarsk, Russia. Retrieved June 27, 2011 from http://risktheory.net/papers/masr2003_1.pdf

Novosyolov, A. (2003). Risk aversion in nonlinear decision-making models. Institute of

Computational Modeling, Krasnoyarsk, Russia. Retrieved June 27, 2011 from http://risktheory.net/papers/masr2003_2.pdf

Novosyolov, A. (2008, December). Measuring risk. Institute of Computational Modeling,

Krasnoyarsk, Russia. Retrieved June 27, 2011 from http://www.gnedenko-forum.org/Journal/2008/042008/RATA_4_2008-17.pdf

- NSTISSAM INFOSEC 1-00. (2000, February). Advisory memorandum for the use of the federal information processing standards (FIPS) 140-1 validated cryptographic modules in protecting unclassified national security systems. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/infosec_1-00.pdf
- NSTISSAM INFOSEC 2-00. (2000, February). Advisory memorandum for the strategy for using national information assurance partnership (NIAP) for the evaluation of commercial off-the-shelf security enabled information technology products. *NIST Publications, Computer Security Division*. Gaithersburg, MD. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/nstissam_infosec_2-00.pdf
- NSTISSI 1000. (2000, April). National information assurance certification and accreditation process. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf
- NSTISSI 4009. (2003, May). National information assurance glossary. Fort Meade, MD. Retrieved June 12, 2011, from <http://staff.washington.edu/dittrich/center/4009.pdf>
- NSTISSI 4011. (1994, June). National training standard for information systems security professionals. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf
- NSTISSI 4015. (2000, December). National training standard for system certifiers. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/nstissi_4015.pdf
- NSTISSI 7003. (1996, December). Protected distribution systems. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/nstissi_7003.pdf
- NSTISSP 11. (2003, July). Fact sheet for the national assurance information acquisition policy. Retrieved June 27, 2011 from http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf

Oladimeji, E., Supakkul, S., Chung, L. (2006). Security threat modeling and analysis: A goal-oriented approach. Retrieved July 23, 2011 from

<http://www.google.com/url?sa=t&source=web&cd=13&ved=0CCQQFjACOAo&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.103.2997%26rep%3Drep1%26type%3Dpdf&rct=j&q=information%20systems%20threat%20profile&ei=HxwpTqi1AerhiAKVvqmwAg&usg=AFQjCNETTG-0RJsPY0WyHbqbr4rdeStiIQ>

Oltsik, J. (2007, July). The information-centric security architecture. Retrieved June 27, 2011

from <http://www.emc.com/collateral/analyst-reports/esg-info-centric-security-architecture.pdf>

OMB Circular A-130. (1985, December). Management of Federal Information Resources.

Retrieved July 31, 2011 from

<http://www.whitehouse.gov/sites/default/files/omb/circulars/a130/a130trans4.pdf>

PDD-63. (1998, May). Critical infrastructure protection. Retrieved June 9, 2011, from

<http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

PMBOK. (2004, January). A guide to the project management body of knowledge. Retrieved

June 27, 2011 from <http://www.pmi.org>

Public Law 100-235. (1988, January). Computer security act of 1987. Retrieved June 27, 2011

from <http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf>

Quantil.com. (2011). An incomplete history of risk management. Retrieved August 31, 2011

from <http://www2.isye.gatech.edu/~brani/isyebayes/bank/handout1.pdf>

- Rainer, R., Snyder, C. (1991). Risk analysis for information technology. *Journal of Management Information Systems*, Vol. 8, No. 1, pp. 129-147. Retrieved June 27, 2011 from <http://paul-hadrien.info/backup/LSE/IS%20490/risk%20analysis%20for%20IT.pdf>
- Ragheb, M. (2011). Risk quantification. Retrieved July 24, 2011 from <https://netfiles.uiuc.edu/mragheb/www/NPRE%20457%20CSE%20462%20Safety%20Analysis%20of%20Nuclear%20Reactor%20Systems/Risk%20Quantification.pdf>
- Renn, O. (1998). A model for an analytic-deliberative process in risk management. *Environmental Science Technology*, Vol. 33 (18), pp 3049-3055. Retrieved July 24, 2011 from <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/26.pdf>
- Risk Assessment. (1993, December). Risk assessment. Methodology Manual, Texas State Auditor's Office. Retrieved July 14, 2011 from http://www.preciousheart.net/chaplaincy/Auditor_Manual/4risk.pdf
- Risk Management Guide for DoD Acquisition. (2006, August). Risk management guide for DoD acquisition. Retrieved June 27, 2011 from <http://www.dau.mil/pubs/gdbks/docs/RMG%20Ed%20Aug06.pdf>
- Roger, C., Petch, J. (1999, April). Uncertainty & risk analysis. PricewaterhouseCoopers. United Kingdom. Retrieved July 14, 2011 from <http://clem.mscd.edu/~mayest/Excel/Files/Uncertainty%20and%20Risk%20Analysis.pdf>
- Rowe, W. (1975). An "anatomy" of risk. Environmental Protection Agency. Washington, D.C. Retrieved July 25, 2011 from http://tobaccodocuments.org/nysa_ti_s1/TI55841556.pdf
- Roy, A. (2010). Attack countermeasure trees: A non-state-space approach towards security and finding optimal countermeasure sets. Retrieved July 31, 2011 from <http://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/3148/thesis.pdf?sequence=1>

Ruszczynski, A., Shapiro, A. (2006, August). Optimization of convex risk functions. *Informs, Mathematics of operations research*. Vol. 31, No. 3. Retrieved July 14, 2011 from

<http://edoc.hu-berlin.de/series/speps/2004-8/PDF/8.pdf>

Rutgears, L., Srivastava, R., Mock, T. (2006). An information systems security risk assessment model under dempster-shafer theory of belief functions. *Journal of Management Information systems*, Vol. 22, No. 4, pp 109-142. Retrieved July 14, 2011 from

<http://paul->

[hadrien.info/backup/LSE/IS%20490/Risk%20assesment%20and%20theory%20of%20belief%20functionis.pdf](http://paul-hadrien.info/backup/LSE/IS%20490/Risk%20assesment%20and%20theory%20of%20belief%20functionis.pdf)

Saaty, T. (1987). Risk – its priority and probability: The analytic hierarchy process. *Risk Analysis*, Vol. 7, No. 2. Retrieved July 24, 2011 from

<http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/24.pdf>

Sandia. (2006). A risk assessment methodology for physical security. Retrieved August 26, 2011 from <http://www.sandia.gov/ram/RAM%20White%20Paper.pdf>

Section 3541 Title 44 U.S.C.. (2002, January). Federal information security management act of 2002. Retrieved June 27, 2011 from

<http://www.csrc.nist.gov/drivers/documents/FISMA-final.pdf>

Sensitivity and Risk Analysis. (1999). Handbook for the economic analysis of water supply projects. Retrieved July 23, 2011 from

http://www.adb.org/documents/handbooks/water_supply_projects/Chap7-r6.PDF

- Sherer, S., Alter, S. (2004, July). Information system risks and risk factors: are the mostly about information systems? Communications of the Association for Information Systems, Vol. 14, pp. 29-64. Retrieved June 27, 2011 from http://www.stevenalter.com/StevenAlter.com/Downloads_files/CAIS%2014-2%20IS%20Risk%20Factors%20-%20Are%20They%20Mostly%20About%20IS.pdf
- Schilling, M. (2009). Strategic management of technology and innovation. Edition 3R. Boston, MA: McGraw-Hill Irwin.
- Spiegel, M., Schiller, J., Srinivasan, R. (2009). Probability and statistics. Schaum's Outline Series.
- SSE-CMM. (2003, June). Systems security engineering capability maturity model. Retrieved June 27, 2011 from <http://www.sse-cmm.org/docs/ssecmmv3final.pdf>
- Startzman, R.A. (1985). An improved computation procedure for risk analysis problems with unusual probability functions. Society of Petroleum Engineers, Texas A&M U. Retrieved July 14, 2011 from http://www.pe.tamu.edu/wattenbarger/public_html/Selected_papers/SPE13772_risk%20analysis.pdf
- Tan, D. (2002). Quantitative Risk Analysis Step-By-Step. SANS Institute. Retrieved July 23, 2011 from http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849
- The Probability Calculus. (2000). Chapter 6: The probability calculus. Retrieved July 23, 2011 from http://fitelson.org/confirmation/skyrms_6.pdf
- Vidakovic, B. (2004). Probability, conditional probability, and bayes formula. Retrieved August 25, 2011 from <http://www2.isye.gatech.edu/~brani/isyebayes/bank/handout1.pdf>