Applying Multi-Criteria Decision-Making Methods to the Department of Defense Cloud Service Offering Security Authorization Process

by Thomas R. Ivan

B.S. in Physical Science, May 1984, United States Naval Academy
M.S. in Information Systems, March 1991, United States Naval Postgraduate School
M.S. in Engineering Management, May 2012, University of South Florida

A Praxis submitted to

The Faculty of
The School of Engineering and Applied Science
of The George Washington University
in partial fulfillment of the requirements
for the degree of Doctor of Engineering

August 31, 2018

Praxis directed by

Stuart Young
Adjunct Professor of Engineering and Applied Science

Thomas Bersson
Adjunct Professor of Engineering and Applied Science

The School of Engineering and Applied Science of The George Washington University certifies that Thomas R. Ivan has passed the Final Examination for the degree of Doctor of Engineering as of July 30, 2018. This is the final and approved form of the Praxis.

Applying Multi-Criteria Decision-Making Methods to the Department of Defense Cloud Service Offering Security Authorization Process

Thomas R. Ivan

Praxis Research Committee:

Stuart Young, Adjunct Professor of Engineering and Applied Science, Praxis Director

Thomas Bersson, Adjunct Professor of Engineering and Applied Science, Committee Member

Amirhossein Etemadi, Assistant Professor of Engineering and Applied Science, Committee Member

Ebrahim Malalla, Visiting Associate Professor of Engineering and Applied Science, Committee Member

Nicholas J. Hoffer, President, InterOptions, LLC / Telecommunications Executive, Committee Member

© Copyright 2018 by Thomas R. Ivan
All rights reserved

Acknowledgments

Thank you to my advisors, Dr. Stuart Young and Dr. Thomas Bersson, for their invaluable feedback, guidance, and time committed to ensure my praxis was successful. I would also like to thank Colonel Nicholas J. Hoffer, USMC (Ret.) for his mentorship throughout my research and my professional and personal endeavors. Thank you to my wife Barbara for her infinite support and patience throughout the time it took to finish the Praxis.

Abstract of Praxis

Applying Multi-Criteria Decision-Making Methods to the Department of Defense Cloud Service Offering Security Authorization Process

Cloud computing offers the potential for the Department of Defense (DoD) to lower its computing costs while making information resources more widely available. Recognizing the potential benefits to the DoD of using cloud computing technologies, the Deputy Secretary of Defense issued a September 2017 memorandum directing an acceleration of the DoD's adoption of cloud computing technologies. This aggressive approach to cloud computing adoption is largely driven by the belief that cloud computing is critical to maintaining the US military's technological advantage over potential adversaries.

Cloud computing offers potential benefits in terms of increased efficiency for information technology (IT) resource utilization along with reduced IT infrastructure procurement and sustainment costs. Along with potential benefits, there are significant security challenges that must be addressed while pursuing the guidance to aggressively increase DoD use of cloud computing technology. The security of data hosted in a cloud computing environment is a critical issue for Government consumers, organizations, and mission owners.

This Praxis produces a decision support model to identify and assess security considerations relevant to issuing an Authority to Operate (ATO) for a cloud computing service offering in DoD organizations. The model uses Multi-Criteria Decision-Making methods to help the mission owner Authorizing Official (AO) make an appropriate security authorization decision.

The Praxis identifies decision criteria, develops weights for the criteria, and builds a model for evaluating cloud service offerings against the weighted security authorization decision criteria. Using this approach, the model produces a consistent and repeatable means for making security authorization decisions for cloud service offerings.

Table of Contents

Acknowledgements iv

Abstract v

Table of Contents vii

List of Figures ix

List of Tables xi

Acronyms xiii

Chapter 1 – Introduction 1

1.1 Scope of the Research 2

1.2 Purpose and Motivation 6

1.3 Problem Statement 8

1.4 Thesis Statement 8

1.5 Research Objective 8

1.6 Research Questions 8

1.7 Hypothesis 9

1.8 Impact of Praxis Research 9

1.9 Praxis Organization 13

Chapter 2- Literature Review 15

2.1 Cloud Computing Definitions and Service Models 15

2.2 DoD Cloud Computing Security Concerns 18

2.3 Addressing Cloud Computing Security Concerns 23

2.4 Multi-Criteria Decision-Making (MCDM) 26

2.4.1 MCDM Methods 26

2.4.2 MCDM Components 28

2.4.3 Using MCDM Methods 30

2.5 Summary 32

Chapter 3 – Methodology 33

3.1 Phase 1: Preliminary Research 34

3.2 Phase 2: Initial Model Development 35

3.3 Phase 3: Data Collection 40

3.3.1 Qualitative Data 40

3.3.2 Quantitative Data 43

3.4 Phase 4: Data Analysis and Model Refinement 45
3.5 Phase 5: Model Run and Results 46
3.6 Phase 6: Validation 48
Chapter 4 – Results 49
4.1 Security Report Data Analysis Results 49
4.2 AHP Criteria Weight Calculation 53
4.2.1 AHP Criteria Weight Calculation; Case 1 54
4.2.2 AHP Criteria Weight Calculation; Case 2 57
4.2.3 AHP Criteria Weight Calculation; Case Comparison 61
4.3 Applying the Weighted Criteria to the Security Authorization Decision Making Process 63
4.4 Validation 68
4.5 Discussion 69
4.5.1 Key Findings 69
4.5.1.1 Criteria Selection and Weighting 69
4.5.1.2 Determining the Acceptance Threshold 70
4.5.1.3 Acceptance Threshold Validation 71
4.5.2 Hypothesis Resolution 72
4.5.3 Limitations 73
4.6 Chapter Summary 74
Chapter 5 – Conclusions 76
5.1 Conclusion 76
5.2 Practical Application 77
5.3 Future Research 77
References 80
Appendix A A-1

List of Figures

Figure 1-1 Praxis Concept Diagram 3

Figure 1-2 Praxis Purpose 7

Figure 1-3 Praxis Impact 11

Figure 1-4 Security Assessment Decision 12

Figure 2-1 Risk Management Framework (RMF) 22

Figure 3-1 Methodology Map 34

Figure 3-2 MCDM Candidate Methods 36

Figure 3-3 Decision Hierarchy 39

Figure 3-4 Qualitative Decision Criteria and Attributes 42

Figure 3-5 Quantitative Data 44

Figure 3-6 Data Collection and Data Analysis Model Phases 45

Figure 3-7 Developing AHP Criteria Weights 47

Figure 4-1 Mapping Security Report Quantitative Data to Decision Criteria 50

Figure 4-2 Security Report Quantitative Data Analysis 51

Figure 4-3 Security Report Data Analysis Results 52

Figure 4-4 AHP Numeric Value Interpretation; Case 1 53

Figure 4-5 AHP Numeric Value Interpretation; Case 2 53

Figure 4-6 Case 1 and Case 2 Comparison 62

Figure 4-7 Calculating Weighted Scores 65

Figure 4-8 CSO Weighted Scores 65

Figure 4-9 CSO Weighted Scores for Ø = 0.85 66

Figure 4-10 CSO Weighted Scores for Ø = 0.9 67

Figure 4-11 CSO Weighted Scores for Ø = 0.95 68

Figure 4-12 Applying Model Results to Security Authorization Decision-Making 75

List of Tables

Table 4-1 AHP Pairwise Comparison Matrix with intensity judgments; Case 1 54

Table 4-2 AHP Column Addition; Case 1 55

Table 4-3 AHP Normalized Matrix; Case 1 55

Table 4-4 Calculated Priorities with Row Averages; Case 1 55

Table 4-5 Results; Original Judgments and Priorities; Case 1 55

Table 4-6 Priorities as Factors; Case 1 56

Table 4-7 Weighted Column Calculation; Case 1 56

Table 4-8 Weighted Sum Calculation; Case 1 56

Table 4-9 λ_{max} calculation; Case 1 56

Table 4-10 Consistency Ratio Calculation; Case 1 57

Table 4-11 AHP Pairwise Comparison Matrix with intensity judgments; Case 2 58

Table 4-12 AHP Column Addition; Case 2 58

Table 4-13 AHP Normalized Matrix; Case 2 59

Table 4-14 Calculated Priorities with Row Averages; Case 2 59

Table 4-15 Results; Original Judgments and Priorities; Case 2 59

Table 4-16 Priorities as Factors; Case 2 59

Table 4-17 Weighted Column Calculation; Case 2 60

Table 4-18 Weighted Sum Calculation; Case 2 60

Table 4-19 λ_{max} calculation; Case 2 60

Table 4-20 Consistency Ratio Calculation; Case 2 61

Table 4-21 CSO Evaluation Matrix 63

Table 4-22 FedRAMP Moderate Controls & Controls Enhancement 64

Table 4-23 CSO Evaluation Results 65

Table 4-24 Rank Order of Evaluated CSOs 66

Table 4-25 CSO Rankings Against Mission Owner Acceptance Threshold 66

Acronyms

AHP	Analytic Hierarchy Process
AO	Authorizing Official
ATO	Authority to Operate
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CR	Consistency Ratio
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDI	Department of Defense Instruction
FedRAMP	Federal Risk and Authorization Management Program
FOUO	For Official Use Only
GAO	Government Accountability Office
IaaS	Infrastructure as a Service
IL	Information Level
IT	Information Technology
MCDM	Multi-Criteria Decision Making
NIST	National Institute of Standards and Technology
NSS	National Security Systems
PaaS	Platform as a Service

PHI	Protected Health Information
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RI	Random Index
RMF	Risk Management Framework
SaaS	Software as a Service
SAW	Simple Additive Weight
SP	Special Publication
SRG	Security Requirements Guide
TOPSIS	Technique for Order Preference by Similarity to Ideal Solution

CHAPTER 1 Introduction

Cloud computing offers a way for the Department of Defense (DoD) to lower its costs of computing resources, improve performance, and make information resources more widely available thereby increasing overall efficiency of information technology investments (IDA Study, 2015). Recognizing the potential benefits to the DoD of using cloud computing technologies, the Deputy Secretary of Defense issued a September 2017 memorandum directing an acceleration of the DoD's adoption of cloud computing technologies because of the belief that cloud computing is critical to maintaining the US military's technological advantage over potential adversaries (Deputy Secretary of Defense Memorandum, 2017).

Though cloud computing offers potential benefits in terms of increased efficiency for information technology (IT) resource utilization, reduced IT infrastructure procurement and sustainment costs, and improved access to data, there are significant challenges that must be addressed to realize the Deputy Secretary of Defense's guidance to aggressively increase the DoD's use of cloud computing technology and resources. The security of data hosted in a cloud computing environment is a critical issue for Government consumers, organizations, and mission owners (IDA Study, 2015).

The Praxis will produce a decision support model to identify and assess security considerations relevant to issuing an Authority to Operate (ATO) for a cloud computing service offering (CSO) in DoD organizations. The model will use Multi Criteria Decision Making (MCDM) to help the organization Authorizing Official (AO) make a security authorization decision.

1.1 Scope of the Research

Praxis research focuses on security authorization decision-making for unclassified DoD information at Information Impact Level 4 (IL 4) and Information Impact Level 5 (IL 5). The concept diagram presented in Figure 1-1 shows praxis focus and impact.

The Start, Data, Process, and Decision components shown in the Praxis Concept Diagram are described in the following paragraphs.

The Start component of the concept diagram represents the first step in the cloud security authorization decision-making process. In this component, data and applications are identified and considered for migration to a cloud computing environment. The praxis focuses on data and applications at IL 4 and IL 5. IL 4 information is Controlled Unclassified Information (CUI) that, under law, requires protection from unauthorized disclosure. Examples are Personally Identifiable Information (PII), Protected Health Information (PHI), and For Official Use Only (FOUO) information (DoD Security Requirements Guide, 2016). IL 5 information is CUI that the data owner deems necessary to protect at a higher level than IL 4 data and includes data that supports unclassified National Security Systems (NSS) (DoD Security Requirements Guide, 2016).

The Data component of the concept diagram represents the Cloud Service Offering (CSO) that is proposed by a Cloud Service Provider (CSP). A CSP is an entity that offers one or more cloud services in one or more deployment models (DoD Security Requirements Guide, 2016). A CSO is the service offering or solution available from the CSP (DoD Security Requirements Guide, 2016). Types of cloud service models and cloud deployment models are described in the Literature Review.

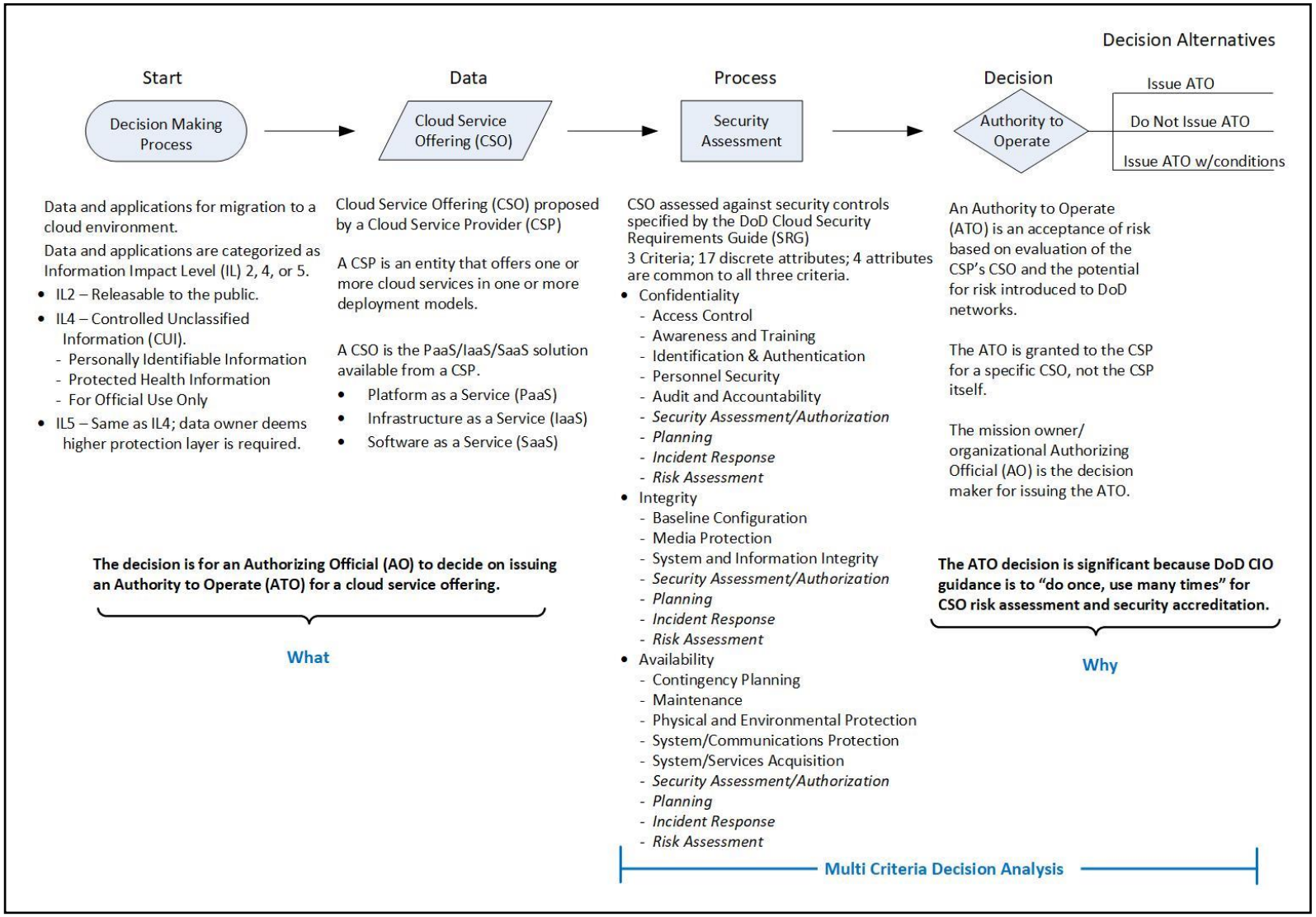

Figure 1-1. Praxis Concept Diagram

In the concept diagram, the CSO is a proposal submitted by a commercial cloud service provider to the DoD for evaluation and consideration for acceptance and authorization. The CSO is most often a procurement-sensitive document that contains proprietary information detailing how the CSP intends to deliver the offering. The CSO can contain technical and cost details whose release is restricted to only those individuals engaged in the formal evaluation process.

The Process component of the concept diagram represents the security assessment that is conducted for the CSO. For the DoD security authorization process, the security assessment is conducted against security controls specified in the DoD Cloud Security Requirements Guide (SRG). Mapping the applicable security controls to security authorization decision criteria is discussed in Chapter 3.

The Decision component of the concept diagram represents the decision alternatives from which the Authorizing Official (AO) can choose. The decision is whether or not to issue an Authority to Operate (ATO) which allows the CSO to access, process, or store IL 4 or IL 5 data and applications. An ATO is an acceptance of risk based on evaluation of the cloud service offering and the potential for risk introduced to DoD networks and data. The ATO is granted to the cloud service provider for a specific offering, not to the cloud service provider itself.

The Decision component is a highly qualitative element of the process and is the primary focus of the praxis. The praxis addresses the qualitative elements by developing a quantitative approach using multi-criteria decision making to remove subjectivity from the cloud security authorization decision-making process.

The Decision component of the process is highly qualitative primarily for the following reasons:

- The security authorization decision is largely influenced by the mission owner's risk tolerance. Risk tolerance is based on the mission owner's assessment of the impact if the confidentiality, integrity, or availability of information is compromised. Different mission owners can have different risk tolerances even though they are using similar information.

  Risk tolerance is determined by the mission owner's expert judgment, experience, and assessment of impact should the information in the cloud computing environment be compromised. These are subjective assessments that can vary widely between DoD organizations and mission owners.
- A standard risk acceptance threshold has not yet been established for DoD organizations to use in their cloud security authorization decision-making processes. Lacking an agreed upon acceptance threshold for risk management, DoD organizations use their Authorizing Official's expert judgment and subjective assessment to either accept or reject a cloud service offering based on the offering's security posture.

Based on the results of the security assessment, the AO has three decision alternatives. The first alternative is to issue an ATO authorizing the cloud service offering to access, process, or store IL 4 and IL 5 data and applications. The second alternative is to not issue an ATO and take no further action with the cloud service offering. The third alternative is for the AO to issue an ATO with conditions that must be satisfied before full authorization is granted. The conditions associated with the cloud service offering

must be mitigated or resolved through a Plan of Action and Milestones (POA&M) submitted by the commercial cloud service provider and approved by the Authorizing Official.

Applying MCDM methods allows the AO to select alternative one, which is to issue an ATO, or to select alternative two, which is to not issue an ATO. MCDM methods remove subjectivity from the authorization decision by introducing a quantitative analysis of relevant security concerns and criteria.

The third decision alternative, which is to issue an ATO with conditions, can be considered a subset of alternative one. MCDM methods can be used to select between alternatives one and two. Decision alternative three allows the AO to use his or her expert judgment and experience to accept the CSO but place conditions that must be satisfied within a designated amount of time or the security authorization will be rescinded. The CSO must exceed the acceptance threshold established by MCDM methods in the praxis for alternatives one or three to be chosen.

The ATO decision is significant because of the DoD Chief Information Officer (DoD CIO) guidance to "do once, use many times" for risk assessments and security accreditation decisions (DoD Chief Information Officer Memorandum, 2014).

1.2 Purpose and Motivation

The purpose of the praxis research is to develop a consistent and repeatable process for DoD Authorizing Officials to conduct security assessments and make security authorization decisions for cloud service offerings. Figure 1-2, which mirrors the Decision component of the concept diagram, shows the purpose of the praxis by

highlighting the potentially arbitrary and inconsistent nature of the current immature cloud security authorization decision-making process.

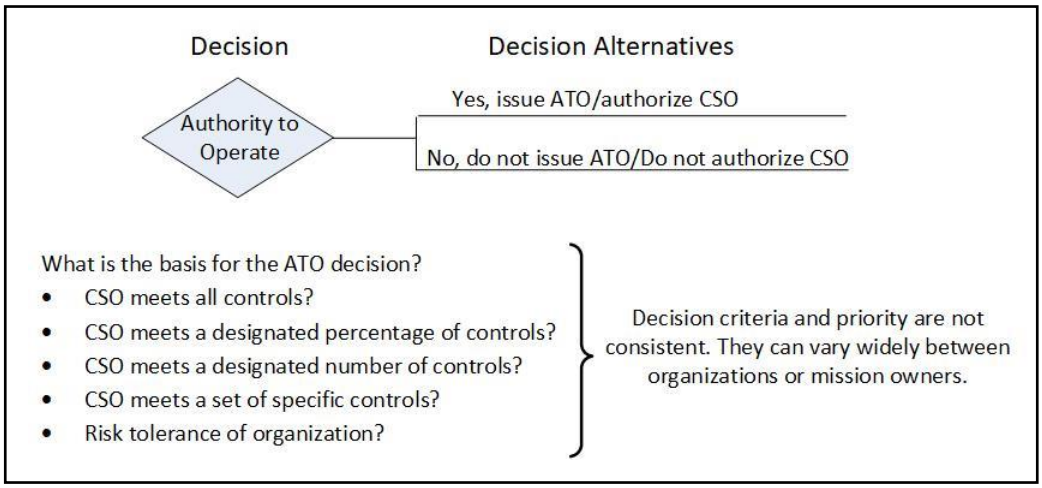

Figure 1-2. Praxis Purpose

The cloud security authorization process is a relatively immature process largely because of the limited number of cloud service offerings that have been assessed and authorized for use on DoD networks. Because of the immaturity, the basis of the authorization decision can vary between mission owners and AOs.

The lack of common decision criteria and priority of the criteria creates an inconsistent and potentially subjective security authorization decision-making process. The motivation for the praxis research is to remove inconsistency and subjectivity in cloud security authorization decision-making. Removing inconsistency and subjectivity in cloud security authorization decision-making reduces the risk potentially introduced to DoD networks, data, and applications by the authorized cloud service offerings.

The decision support model developed in the praxis can be immediately and directly applied by DoD Authorizing Officials and security engineers as a component of the cloud security authorization decision-making process.

1.3 Problem Statement

The current inconsistent and subjective cloud security authorization decision-making process, which uses equally weighted criteria and a Yes/No checklist of security controls, introduces risk to DoD information that is accessed, processed, or stored in a cloud computing environment.

1.4 Thesis Statement

Multi criteria decision making (MCDM) methods using weighted decision criteria can increase the consistency, repeatability, and objectivity of cloud service offering security authorization decision making.

1.5 Research Objective

The formal objective of this research is to develop a consistent and repeatable process using weighted decision criteria for DoD Authorizing Officials to make cloud service offering security authorization decisions.

1.6 Research Questions

The praxis aims to answer the following questions regarding the DoD security authorization decision making process for cloud service offerings:

- Can cloud computing security authorization decision criteria be identified?
- What cloud computing security authorization criteria can be quantified?
- How can cloud computing security authorization criteria be quantified?
- Can statistical analysis be used to develop weighted decision criteria?

- Can the cloud computing security authorization process be made more objective, consistent, and repeatable?

1.7 Hypothesis

The research objectives and questions translate into the following hypothesis:

$H1_0$: Multi criteria decision making methods using weighted decision criteria cannot increase the consistency, repeatability, and objectivity of cloud service offering security authorization decision making.

$H1_a$: Multi criteria decision making methods using weighted decision criteria can increase the consistency, repeatability, and objectivity of cloud service offering security authorization decision making.

1.8 Impact of Praxis Research on the Cloud Security Authorization Decision-Making Process

The impact of praxis research on the cloud security authorization decision making process is shown in Figure 1-3 and described in this section. The praxis research increases the consistency, objectivity, and repeatability of the current cloud computing security authorization decision making process by identifying weighted decision criteria and establishing an acceptance threshold for issuing an ATO.

The components of the security authorization decision-making process impacted by the praxis are discussed in the below paragraphs. The impact of the praxis on the Process and Decision components produces a more consistent decision-making process which can be immediately applied by DoD Authorizing Officials and security engineers as part of the cloud service offering security assessment and decision-making process.

The Data component shown in Figure 1-3 is the same for the current security authorization decision-making process and for the process developed in the praxis. The

Data component represents a cloud service offering that is not yet authorized for introduction to DoD networks, data, or applications.

The praxis primarily impacts the Security Assessment and Decision components of the cloud security authorization decision-making process. Figure 1-4 shows how the praxis impacts these two components.

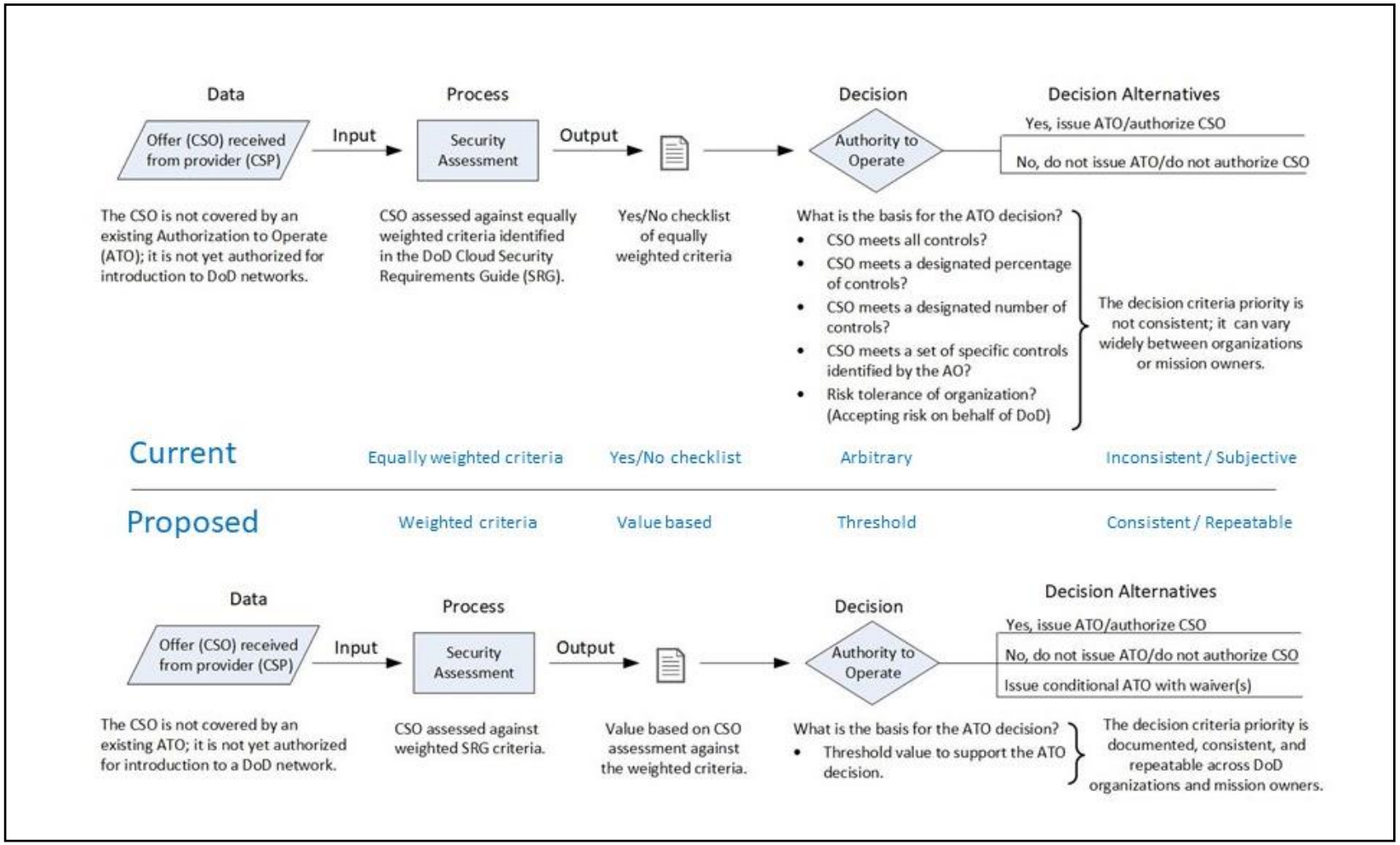

Figure 1-3. Praxis Impact

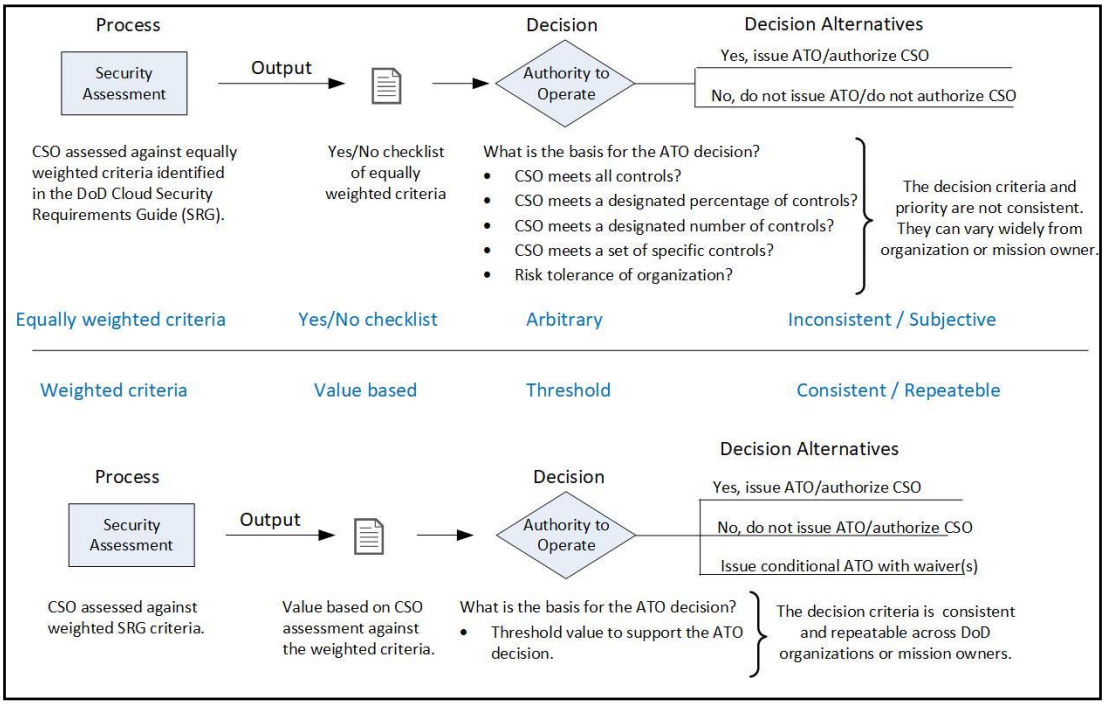

Figure 1-4. Security Assessment and Decision

The current security authorization process, shown in the top portion of Figure 1-4, uses equally weighted criteria from the DoD SRG. In the SRG, the criteria are listed as security controls. The equally weighed criteria are evaluated using a Yes/No method to produce a checklist of criteria that are either satisfied or not satisfied. The checklist produced from the security assessment is the basis for the authorization decision.

The authorization decision in the current process can be based on several factors whose relative importance is determined by the Authorizing Official. The factors upon which the authorization decision is made can be:

- The offering meets all security controls.
- The offering meets a designated percentage of controls as determined by the AO.
- The offering meets a designated number of controls as determined by the AO.

- The offering meets a specific set of controls as determined by the AO.

Because each organization or mission owner Authorizing Official has the ability to apply any or all of the above criteria, the security authorization can be applied inconsistently across DoD organizations.

The security authorization process developed in the praxis, shown in the bottom portion of Figure 1-4, uses weighted criteria against which the cloud service offering can be assessed. The weighted criteria assessment produces a value rather than a Yes/No checklist as the basis for the security authorization decision. The praxis also develops a threshold value below which the Authorizing Official will not consider issuing an Authority to Operate to the cloud service offering.

Establishing and applying weighted criteria and an acceptance threshold produce a consistent and repeatable process that can be immediately applied by Authorizing Officials and security engineers to in-process and planned cloud service offering security authorization decisions.

1.9 Praxis Organization

The praxis is organized into five chapters. Chapter 1 introduces the research scope, problem statement, research objectives and questions, hypothesis, and impact of the praxis.

Chapter 2 is a literature review of research performed relevant to cloud computing security, multi criteria decision making, and DoD security authorization decision making process.

Chapter 3 presents the praxis Methodology. Model results and discussions are presented in Chapter 4. Conclusions and future research opportunities are presented in Chapter 5.

CHAPTER 2 Literature Review

The study of cloud computing security is a high priority for DoD organizations because of the potentially significant impact should the confidentiality, integrity, or availability of information accessed, processed or stored by cloud computing technology be compromised. A critical part of cloud computing security is the completeness and rigor of the process leading to a security authorization decision for a cloud service offering. Before connecting to a DoD network for the purpose of accessing, processing, or storing DoD sensitive information, the cloud service offering must be assessed against existing and emerging security guidance. The results of the assessment are the basis for the security authorization decision.

The mission owner Authorizing Official (AO) is responsible for making the security authorization decision which, depending on the cloud deployment model, can impact organizations and data beyond that under the mission owner's control. Guidance to help the AO make an appropriate security authorization decision continues to mature with frequent updates to requirements and security control publications. Understanding the cloud computing service models, cloud computing deployment models, and the factors impacting cloud computing security is critical for the AO to make an appropriate security authorization decision.

2.1 Cloud Computing Definitions and Service Models

Because cloud computing offers federal agencies a means to potentially procure required information technology services faster and possibly cheaper than through traditional procurement methods, the growth in cloud computing utilization is expected to rapidly increase. Growth estimates from the U.S. Government Accountability Office

(GAO) report that federal agencies spent more than $2 billion on cloud computing services in fiscal year 2016 and expect to spend more in future years (GAO Report on Cloud Computing, 2016).

The National Institute of Standards and Technology (NIST) defines cloud computing as a means for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resource that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST SP 800-145, 2001). The DoD Cloud Security Requirements Guide "adheres to the NIST definition to characterize and standardize the discussion of cloud computing" (DoD SRG, 2016).

Cloud computing delivers a range of options for computing infrastructure, software development platforms, or services that are available through an on-demand model. These options, called service models, are known as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Vaquero, 2009). DoD mission owners are looking to employ all three cloud service models across a range of data and applications.

The service model definitions used within the DoD are presented in the NIST Framework for Cloud Usability, Special Publication 500-316:

- SaaS provides consumers the use of applications in the cloud. The consumer does not control or manage the applications or the environment in which they run.
- PaaS provides consumers the ability to deploy applications created or acquired by the consumer using programming languages, libraries, services, or tools supported by the cloud service provider. The consumer does not manage or control the cloud infrastructure but has control over the deployed applications.

- IaaS provides consumers with the ability to provision processing, storage, networks, and other computing resources where the consumer is able to deploy and run arbitrary software which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications (NIST Framework for Cloud Usability, 2015).

Cloud computing service offerings are delivered through one of four standard deployment models. The models are public, private, community, and hybrid. The primary difference between the four models is where the hosting hardware and infrastructure is found and what organization is responsible for maintaining the cloud ecosystem (Congressional Research Service, 2015).

The four cloud computing deployment models are defined as:

- Public clouds are provided by a cloud service provider and offer a multi-tenant shared operating environment (Prakash, 2016). Public clouds have increased concerns on security and privacy because their design potentially allows multiple consumers to access the same cloud instance (IDA Study, 2015).
- Private clouds are provided by a cloud service provider and offer a single-tenant dedicated operating environment (Prakash, 2016). Because private clouds are operated solely for the acquiring organization their cost can equal the cost for operating a dedicated data center (IDA Study, 2015).
- Community clouds are provided by a cloud service provider and offer single-tenant or multi-tenant operating environments for a specific community of interest (Prakash, 2016).

- Hybrid clouds combine features of public and private cloud service offerings for the purpose of facilitating information exchange and application portability across different cloud service offerings and cloud service providers (Prakash, 2016).

Along with the promise of increased information technology efficiencies with reduced infrastructure costs, cloud computing also presents unique security concerns and threats for both commercial industry and DoD consumers.

The primary inhibitors of more rapid cloud computing adoption and use are concerns for information privacy and security (Chen, 2012). The absence of a mechanism to efficiently evaluate privacy and security concerns is a major barrier to cloud adoption (Daniel, 2013).

Similar to other industries, security concerns for data confidentiality, integrity, and availability are significant factors behind security authorization decisions for cloud service offerings to access, process, or store sensitive DoD information resources.

2.2 DoD Cloud Computing Security Concerns

A review of DoD cloud computing security concerns was performed as part of the praxis literature review. The review included numerous publications, instructions, and reports focused on DoD security concerns and requirements for evaluating and authorizing cloud service offerings. Attention was focused on cloud security concerns for DoD implementations, cloud service offering security accreditation, and identifying decision criteria and the relationship between the identified criteria. This section of the literature review discusses DoD cloud computing security concern findings and observations.

The deployment models and technologies behind cloud computing offerings present different types and levels of risk than traditional on-site information technology infrastructure and services (CSA, 2009). Along with the benefits provided by cloud computing technologies, there is significant concern about the security of information hosted in cloud computing environments. Security of the data accessed, processed, or hosted in the cloud computing environment is the main obstacle to the adoption of cloud computing (Grobauer, 2010).

The security of sensitive data hosted in a cloud computing environment is a rapidly growing concern. The study of cloud computing security, defined as "a set of procedures and measures taken to implement the security of data saved in the cloud", is an emerging focus of study in the computer science discipline (Agarwal, 2016).

The Deputy Secretary of Defense memorandum issued in September 2017 recognizes the potential benefits to the DoD of using cloud computing technologies and directs an acceleration of the DoD's adoption of cloud computing technologies. The acceleration was directed because of the belief that cloud computing is critical to maintaining the US military's technological advantage over potential adversaries (U.S. Deputy Secretary of Defense Memorandum, 2017).

Several studies and reports, published both before and after release of the Deputy Secretary of Defense memorandum, identify security as the primary concern for the DoD's use of cloud computing technology and service offerings. A November 2015 comprehensive study of in-place and planned DoD cloud computing implementations found that while cloud computing presents opportunities to scale computing, realize

efficiencies, and transform IT procurement, there are security concerns on the confidentiality and integrity of data in a cloud computing environment (IDA Study, 2015)

The initial version of the DoD Cloud Security Requirements Guide was published in 2016 to provide guidance and establish requirements for DoD mission owner use of commercial cloud services (DoD Cloud Security Requirements Guide, 2016). The foundation of the Cloud Security Requirements Guide is the belief that the overall DoD's success in meeting its cloud computing objectives depends "upon well executed security requirements, defined and understood by both the DoD and industry partners" (DoD Cloud Security Requirements Guide, 2016).

Decision criteria appropriate for the cloud service offering security authorization decision are confidentiality, integrity, and availability (CNSSI No. 1253, 2009). Cloud computing security is dependent on confidentiality, integrity, and availability which are significant concerns for cloud service providers and data owners using the cloud service offering (Madhubala, 2015).

The definitions for the cloud service offering security authorization decision criteria are presented below and discussed in Chapter 3:

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- Integrity – guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- Availability – ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information on an information system (CNSSI No. 4009, 2015).

Security controls can be mapped to individual decision criteria with a number of security controls common to either two or all three decision criteria (DoD Cloud Security Requirements Guide, 2016).

Federal Risk and Authorization Management Program (FedRAMP) guidance for cloud service offering security authorizations allows a DoD Agency Authorizing Official (AO) to conduct a security assessment and, if appropriate, issue an Authority to Operate (ATO) for the cloud service offering. The ATO is issued for a specific cloud service offering, not the cloud service provider at large (FedRAMP Agency Authorization Roles & Responsibilities, 2017).

FedRAMP guidance limits the Agency-granted authorization only to that Agency's data and that Agency's use of the assessed cloud service offering. The FedRAMP guidance allows the Agency to align any specific security requirements it may have with the overarching FedRAMP requirements and authorization procedures (FedRAMP Agency Authorization Playbook, 2017).

The requirements for issuing an Agency ATO for a cloud service offering are published in the DoD Cloud Security Requirements Guide.

The current security authorization decision-making process uses equally weighted criteria to support the authorization decision. Because the security authorization decision for a cloud service offering can be based on different considerations for different mission

owner Authorizing Officials, the decision criteria priority may not be consistent across DoD cloud service offering security authorization assessments and decision-making processes. This results in a potentially inconsistent application of the security authorization process across DoD mission owners. The decision criteria priority can vary widely between DoD organizations or mission owners.

In addition to the DoD Cloud Security Requirements Guide and FedRAMP publications, the Authorizing Official is given security authorization decision-making guidance in Department of Defense Instruction (DoDI) 8510.01. This Instruction specifies how the Risk Management Framework (RMF) is applied to the security authorization decision-making process during the assessment and post-authorization phases of the cloud service offering's lifecycle. The six-step RMF process is shown in Figure 2-1.

Two important components of DoDI 8510.01 are the requirement for continuous monitoring and the concept of cybersecurity reciprocity.

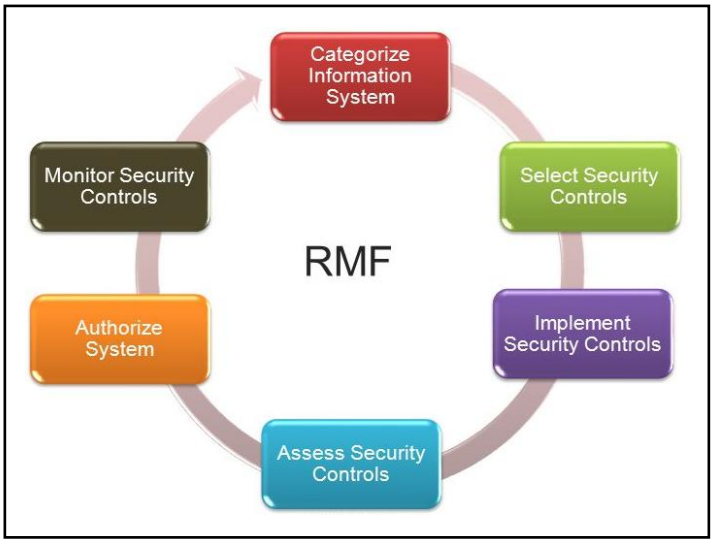

Figure 2-1. DoD Risk Management Framework (Source: DoDI 8510.01)

Continuous monitoring is Step 6 of the RMF process. Continuous monitoring is intended to ensure that the cloud service offering remains in compliance with the security controls against which it was assessed during the authorization process. Continuous monitoring also ensures that any new security controls added since the cloud service offering was authorized are evaluated for applicability and then incorporated into the authorization package if appropriate. A secondary continuous monitoring goal is to identify security-relevant events that negatively affect the security posture of the cloud service offering (DoDI 8510.01).

The concept of cybersecurity reciprocity "is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DoD Information Enterprise" (DoDI 8510.01). Reciprocity is defined as a mutual agreement between parties to accept each other's security assessments to reuse information resources or accept the other's security assessment to facilitate rapid system development and fielding (CNSSI No. 4009). Reciprocity is a critical element in the cloud service offering security authorization decision-making process because of DoD CIO guidance to "do once, use many times" for risk assessments and security accreditations.

2.3 Addressing Cloud Computing Security Concerns

A significant amount of research has been conducted to identify cloud computing security concerns and potential threats to information that is accessed, processed, or stored in a cloud computing environment. This research has focused on identifying potential threats in each cloud service model and in each cloud deployment model. However, little research has been conducted to develop a method for weighting, prioritizing and mitigating the identified threats and security concerns.

One proposed approach to identifying cloud computing security concerns is to group threats into three areas (Barakovic, 2016). These three areas are policy and organizational, technical, and data protection. The data protection area is where the majority of research relevant to the praxis has been conducted. Data protection risks relate to threats to information accessed, processed, or stored in a cloud computing environment.

The primary risks to data processed or stored in a cloud computing environment are:

- Lack of availability to the data by the owner or authorized users.
- Lack of integrity due to resource sharing and weak or inadequate data protections mechanisms such as weak or no encryption.
- Lack of confidentiality due to weak or missing authentication mechanisms (Barakovic, 2016).

A "taxonomy of fears" for cloud computing security developed in 2013 shows the top five security concerns of cloud computing data owners and users as:

- Confidentiality, which is defined as the fear of loss of control over data processed or stored in a cloud computing environment.
- Integrity, which is defined as fear for the correctness of data computation.
- Availability, which is defined as fear of denial of service, especially for data and applications that are considered as mission critical.
- Measuring security capabilities in a manner that allows security concerns to be identified, prioritized, and addressed.
- Measuring regulatory compliance for the cloud service provider chosen to host and process the organization's data and applications (Aruna, 2013).

Threats to data confidentiality, integrity, and availability are consistently identified in research as among the primary reasons why cloud computing adoption has not grown as rapidly as predicted (Chen, 2012). Choosing the appropriate cloud service model and cloud deployment model is largely based on understanding risks to confidentiality, integrity, and availability (Madhubala, 2015).

Prakash proposes a model for addressing security concerns that categorizes the security concerns into three groups. The groups are deployment model issues, service model issues, and network issues (Prakash, 2016). Data confidentiality and data integrity are addressed within the deployment model and service model categories. Data availability is addressed in the network issue category. This research categorizes the security threats to help develop mitigating approaches but does not propose mitigation approaches or techniques.

In a proposed framework for ranking cloud service provider selection criteria, Zoie includes security and privacy as among seven criteria for consideration of cloud service offerings. Security and privacy criteria are designed to "indicate the effectiveness of a service provider in controlling access to services, service data, and physical facilities from which services are provided" (Zoie, 2016). The framework propose in this research identifies security concerns but does not address how the concerns can be prioritized, weighted, and integrated into a decision-making process.

For DoD cloud service offering security assessments and authorization decisions, the current process is relatively immature largely because of the limited number of cloud service offerings that have been assessed and authorized for use on DoD networks.

Because of the immaturity, the basis of the authorization decision, and the degree of risk that is accepted, varies between mission owners and AOs.

The lack of common decision criteria and priority of the criteria creates an inconsistent and potentially subjective security authorization decision-making process. Researching and developing a model using weighted decision criteria removes inconsistency and subjectivity in DoD cloud security authorization decision-making. This reduces the risk potentially introduced to DoD networks, data, and applications by the authorized cloud service offerings.

2.4 Multi-Criteria Decision-Making

Multi-Criteria Decision Making (MCDM) is a method to help make a decision where there are multiple available alternatives with each alternative having several attributes (Yoon, 1995). Multi-Criteria Decision Analysis (MCDA), which is a type of MCDM, consists of approaches and techniques with the goal of generating a ranking of available options from the most to least preferred option (Multi-Criteria Analysis, 2009). Evaluating cloud security offerings is a multi-criteria problem because there are multiple decision criteria that must be considered and ranked (Halabi, 2017).

2.4.1 MCDM Methods

Several MCDM methods have been developed and are used in a wide range of decision-making scenarios. Each method has strengths and weaknesses that influence the type of decision-making environment for which its application is appropriate.

The most common MCDM methods used today, with a short description of each, are:

- Weighted Sum Model (WSM). The Weighted Sum Model is designed for single-dimensional decision-making problems. In these single-dimensional cases, WSM can be applied to identify a preferred solution. WSM is a value measurement MCDM method with criteria assigned a weight to represent its relative importance for comparison to other decision criteria (Tscheikner-Gratl, 2017). WSM is not suited for multi-dimensional decision-making problems because of its design limitation for addressing multiple criteria (Triantaphyllou, 1998). For this reason, WSM is not an appropriate MCDM method for complex multi-criteria decision-making scenarios like the cloud computing security authorization decision-making problem addressed in this praxis.
- Weighted Product Model (WPM) is similar to WSM but uses multiplication rather than addition to calculate the sum. WPM is suitable for single and multi-dimensional decision-making problems, especially maximization problems where the solution sought is that one with the largest value relative to the other candidate solutions (Triantaphyllou, 1998).
- Simple Additive Weighting (SAW). Simple Additive Weight is one of the most frequently used multi-attribute decision making techniques. SAW is based on a weighted average using the arithmetic mean (Adriyendi, 2015). SAW suitability to the cloud security offering security authorization decision-making process is discussed in Chapter 3.
- Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). TOPSIS is a MCDM method based on the concept that the alternative chosen

should be the one having the shortest distance from the ideal solution and furthest distance from the negative ideal solution (Gavade, 2014). TOPSIS is a goal, aspiration, and reference model measuring how an alternative reaches established aspirations or goals (Tscheikner-Gratl, 2017). TOPSIS suitability to the cloud security offering security authorization decision-making process is discussed in Chapter 3.

- Analytic Hierarchy Process (AHP). The Analytic Hierarchy Process decomposes complex multi-criteria decision-making problems into hierarchical relationships between the decision criteria and their attributes (Triantaphyllou, 1998). AHP allows the decision-maker to view the decision in terms of a hierarchy of criteria (Yoon, 1995). Similar to WSM, AHP is a value measurement MCDM method with criteria assigned a weight to represent its relative importance for comparison to other decision criteria (Tscheikner-Gratl, 2017).

  AHP is designed to consider qualitative and quantitative criteria when building decision criteria and developing criteria weights (Gani, 2014). The AHP decision criteria for the cloud security authorization decision-making problem are presented and discussed in Chapter 3.

2.4.2 MCDM Components

Though different in their design and application to decision-making scenarios, MCDM methods share several common characteristics. The common characteristics of MCDM methods, with a short description, are:

- The decision context must be identified. The decision that must be made, the decision maker, and key contributors are identified as the first step in the MCDM process (Multi-Criteria Analysis, 2009).
- Decision options are identified but are not yet assessed or evaluated for suitability. Decision options identified during this step are assessed against the weighted decision criteria as the MCDM process is applied. Decision options can be the selection of the most appropriate solution or elimination or one or more candidate solutions from further evaluation and consideration.
- Decision criteria and the relationship between the criteria are identified. The relevance of the criteria to each identified option is also identified during this step (Multi-Criteria Analysis, 2009). The decision criteria are those factors against which the potential solutions are evaluated for acceptance or rejection.
- Weights are developed for each of the decision criteria. The weights are developed to establish the relative importance of the criteria when evaluated against each other.

  The weights can be developed through qualitative methods, quantitative methods, or a combination of both methods. The decision criteria weights are applied during the evaluation of potential solutions to create a rank order of all evaluated solutions.
- Each option is assessed against the criteria and assigned a value using the criteria weights developed in the previous step (Multi-Criteria Analysis, 2009).

- Options are rank ordered to help the decision-maker either select one option or eliminate one or more options from further consideration (Multi-Criteria Analysis, 2009).

2.4.3 Using MCDM Methods

Because MCDM methods incorporate mathematical and computational tools to weight and assess decision options, they are well-suited for application to complex, multi-dimensional decision-making scenarios (Gani, 2014). The DoD cloud service offering security authorization decision-making environment is a complex, multi-dimensional environment.

The goal of a decision-making process "is to provide the decision maker with the ability to look into the future, and to make the best possible decision based on past and present information and future predictions" (Georgiadis, 2013). MCDM methods accomplish this goal by considering quantitative data, qualitative data, and subjective expert judgment to assess and rank decision options from which the decision-maker can select the best option (Georgiadis, 2013).

MCDM methods are used as components of a decision-making process. The MCDM methods integrate quantitative and qualitative data analysis as components of the decision-making process.

MCDM methods align closely, and are appropriately applied, to a decision-making process with the below characteristics:

- Decision objectives are identified. A decision results from comparing one or more alternatives against one or more criteria relevant to the decision-making environment (Foote, 2010).

- Decision options available to the decision-maker are identified.
- Decision criteria upon which the decision will be made are identified.
- Decision criteria weights are developed for use in evaluating and comparing decision alternatives. The weights can be developed using a combination of quantitative and quantitative data sources.
- Decision options are evaluated against the weighted criteria. Each option is evaluated against the weighted decision criteria independent of the other decision options.
- Decision options are rank ordered to help the decision-maker either choose the most appropriate alternative or to eliminate one or more alternatives from further consideration.
- A decision is made by selecting the most appropriate alternative from among the list of ranked alternatives.

By integrating quantitative and qualitative data analysis into the decision-making process, MCDM methods strengthen an organization's decision-making process by:

- Removing subjectivity in decision criteria weight assignments. In MCDM methods, decision criteria weights are assigned using formal techniques.
- Improving documentation and communication of all components of the decision-making process. MCDM methods facilitate documentation and communication between the decision-maker and stakeholders impacted by the decision.
- Calculation and analysis of the decision criteria weights and alternative rankings generates a documented audit trail for later analysis or refinement as appropriate (Multi-Criteria Analysis, 2009).

The cloud security authorization decision-making process is a multi-criteria environment where MCDM methods can be applied to identify decision goals, identify decision criteria, develop decision criteria weights, and assess available options against the weighted criteria to help the decision-maker select the most appropriate option.

2.5 Summary

For cloud computing to become a key technology enabler with widespread adoption, the risks associated with processing and storing data and applications in a cloud computing environment must be critical parts of an organization's risk management strategy (Elena, 2015).

A significant amount of research has been done to identify and describe threats to the confidentiality, integrity, and availability of information processed or stored in a cloud computing environment. However, little research has been done to develop means for weighting and prioritizing the security concerns so that the decision-maker can make a well-informed security authorization decision.

A quantitative approach to security authorization decision-making that represents cloud computing environment characteristics has not been developed (Teuteberg, 2012). A quantitative method to identify, weight, prioritize, and assess cloud computing security concerns will reduce the level of potential risk introduced to DoD networks and information by cloud service offerings. Multi-Criteria Decision Making (MCDM) methods are proven effective in addressing complex real-world scenarios such as cloud computing service offering security authorization decision making (Gani, 2014).

CHAPTER 3 Methodology

The praxis applies Multi Criteria Decision Making (MCDM) methods to the DoD security authorization decision making process for cloud service offerings. The research scope is for PII, PHI, and FOUO information and applications which are categorized as IL 4 and IL 5 by the DoD Security Requirements Guide.

Before a cloud service offering can connect to a DoD network and access, process, or store IL 4 or IL 5 information, it must receive an Authority to Operate (ATO) from the mission owner Authorizing Official (AO). The current cloud security authorization decision making process uses equally weighted criteria and a Yes/No checklist of security controls which, based on mission owner risk tolerances, can produce inconsistent and subjective outcomes. Applying MCDM methods to the cloud security authorization decision making process produces weighted decision criteria and a value-based threshold for making the security authorization decision. Applying MCDM to the security authorization decision making process makes the process consistent and repeatable for application across a wide range of DoD mission owners.

This chapter describes the Praxis methodology. Figure 3-1 shows the five phases in the methodology and how they are related. Each phase of the methodology is described following Figure 3-1.

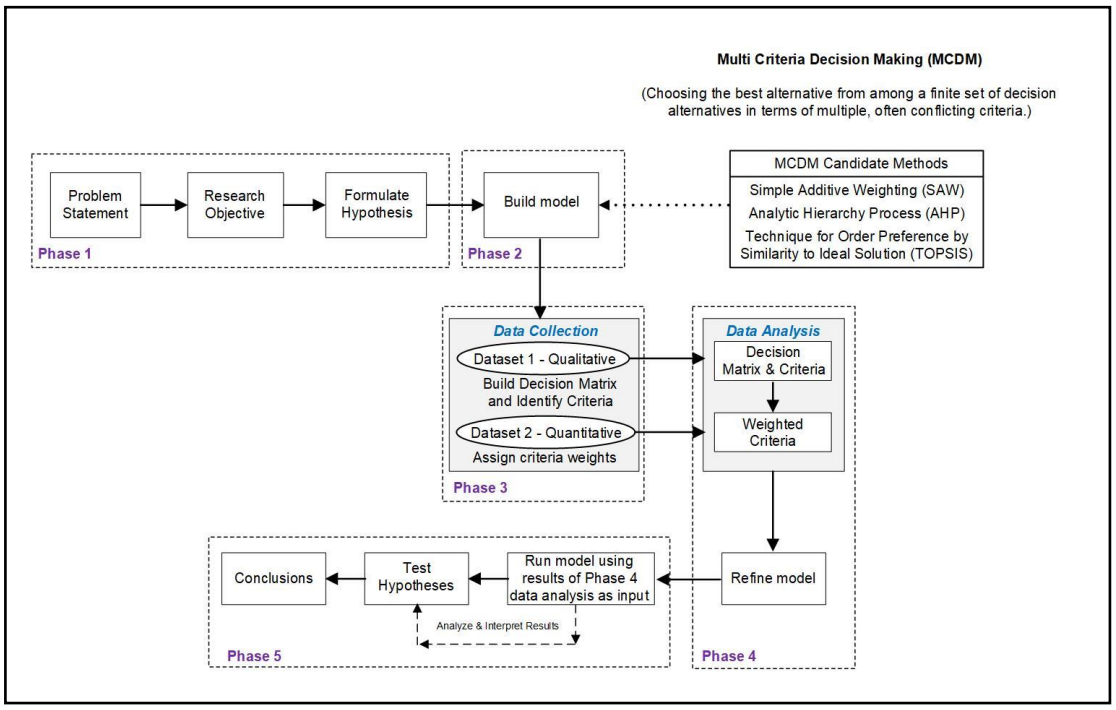

Figure 3-1. Methodology Map

3.1 Phase 1: Preliminary Research

Phase 1, shown in Figure 3-1, focuses on researching and developing the problem statement, research objectives, research questions, and hypotheses. Preliminary research focuses on the current DoD decision making process for cloud service offering security authorizations. Data sources supporting Phase 1 research include direction and guidance published by the DoD Chief Information Officer (CIO), DoD Cloud Security Requirements Guide (SRG), the Defense Information Systems Agency (DISA), and the Federal Risk and Authorization Management Program (FedRAMP).

Phase 1 preliminary research supports the appropriateness of Multi Criteria Decision Making (MCDM) methods to the cloud security authorization decision making process. MCDM represents a collection of decision-making methods for comparing, ranking, and

choosing between multiple alternatives (Gani, 2014). MCDM methods are well suited to choosing the best alternative from among a finite set of decision alternatives with multiple criteria (Yoon, 1995). Choosing the best alternative using weighted decision criteria from among a finite set of decision alternatives accurately describes the cloud service offering security authorization decision making process.

Several MCDM approaches were considered in Phase 2. The candidate MCDM methods are discussed in Section 3.2

3.2 Phase 2: Initial Model Development

Phase 1 outputs were used to build the initial model in Phase 2. The initial model developed in this phase focuses on the problem statement, research questions, and hypotheses formulated during Phase 1.

Outputs from Phase 1 research used to build the model are identification of the security authorization decision making process, security authorization decision alternatives, and decision criteria appropriate for the CSO security authorization decision.

Phase 1 research identified the security authorization decision alternatives as:

- Issue an Authority to Operate (ATO) allowing the cloud service offering to access, process, or store IL 4 and IL 5 information.
- Not issue an ATO thereby prohibiting the cloud service offering from accessing, processing, or storing IL 4 or I L5 information
- Issue an ATO with conditions or restrictions. All conditions must be addressed to the AO's satisfaction in a Plan of Action and Milestones (POA&M) before the cloud service offering is allowed to access, process, or store IL 4 or IL 5 information.

Decision criteria identified in Phase 1 appropriate for the CSO security authorization decision are confidentiality, integrity, and availability (CNSSI No. 1253, 2009). The definitions for these criteria used in the Praxis are:

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- Integrity – guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- Availability – ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information on an information system (CNSSI No. 4009, 2015)

During Phase 2, several candidate MCDM methods were considered for appropriateness and suitability for the praxis model. Candidate MCDM methods considered during this Phase are identified in Figure 3-2 and discussed in the paragraphs following the figure.

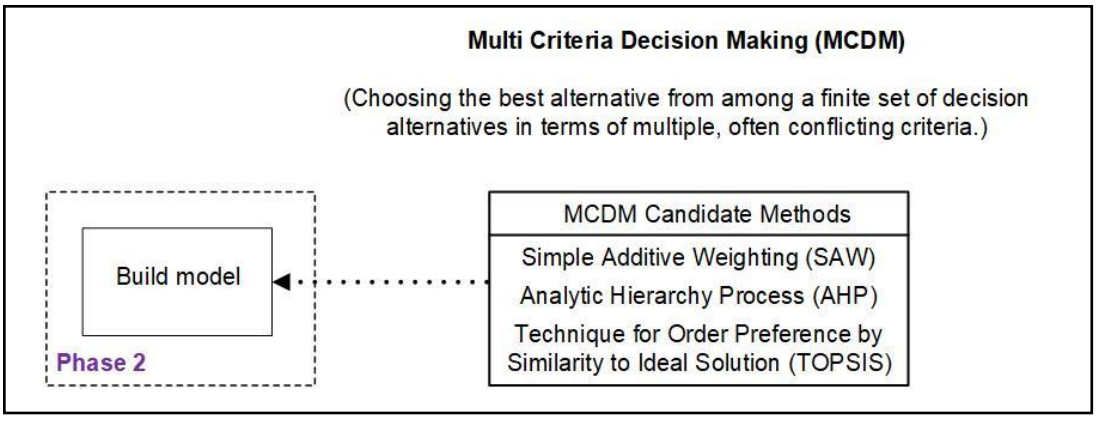

Figure 3-2. Candidate MCDM Methods

MCDM methods considered for the cloud service offering security authorization decision-making process are:

- Simple Additive Weighting (SAW). Simple Additive Weight is one of the most frequently used multi-attribute decision making techniques. SAW is based on a weighted average using the arithmetic mean (Adriyendi, 2015).

  SAW is based on simple addition of scores assigned to different criteria associated with accomplishing the goal of the decision-making process (Velasquez, 2013). Though SAW calculations are simple and do not require complex computer algorithms or programs, the estimates produced with SAW do not always reflect the real situation for which the estimates will be applied (Velasquez, 2013). This is because of the underlying assumption that decision criteria are preferentially independent to each other (Yoon, 1995). Depending on the security authorization decision maker's risk tolerance, the decision criteria of confidentiality, integrity, and availability may not satisfy the preferentially independence condition of SAW. SAW was not chosen for the praxis model primarily for this reason.

- Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). TOPSIS is a MCDM method based on the concept that the alternative chosen should be the one having the shortest distance from the ideal solution and furthest distance from the negative ideal solution (Gavade, 2014). The ideal and negative ideal solutions are unique to the decision that must be made and can be based on quantitative or qualitative factors.

TOPSIS has two limiting factors that impact its suitability and appropriateness for the praxis model.

The first limiting factor of TOPSIS for praxis application is that the method's use of distance from the ideal and negative ideal solutions does not consider the potential correlation of decision attributes. Lack of attribute correlation makes it difficult to weight attributes while maintaining consistency of judgment, especially if the number of decision-making attributes increases (Velasquez, 2013).

The second limiting factor of TOPSIS is that it can give unreliable results because it does not consider uncertainty in attribute weightings (Gavade, 2014). TOPSIS was not chosen for the praxis model primarily for the above two reasons.

- Analytic Hierarchy Process (AHP). AHP is a MCDM method that reduces complex decisions to a series of pairwise comparisons which allow the decision maker to establish priorities to support the decision-making process (Mocenni, 2013.) AHP establishes weights for decision criteria which are then applied to evaluate and prioritize decision alternatives (Mocenni, 2013).

  AHP is well-suited to the security authorization decision-making process primarily because of its ability to create a decision hierarchy identifying the decision objective, decision criteria, decision criteria weights, and decision alternatives (Yoon, 1995).

  For the praxis decision hierarchy, the goal is to make a security authorization decision. The decision criteria are confidentiality, integrity, and

availability. The decision alternatives are to authorize the cloud service offering, not authorize the cloud service offering, or to issue a conditional authorization with conditions that must be satisfied before full authorization is granted. Figure 3-3 shows the AHP decision hierarchy developed for the praxis.

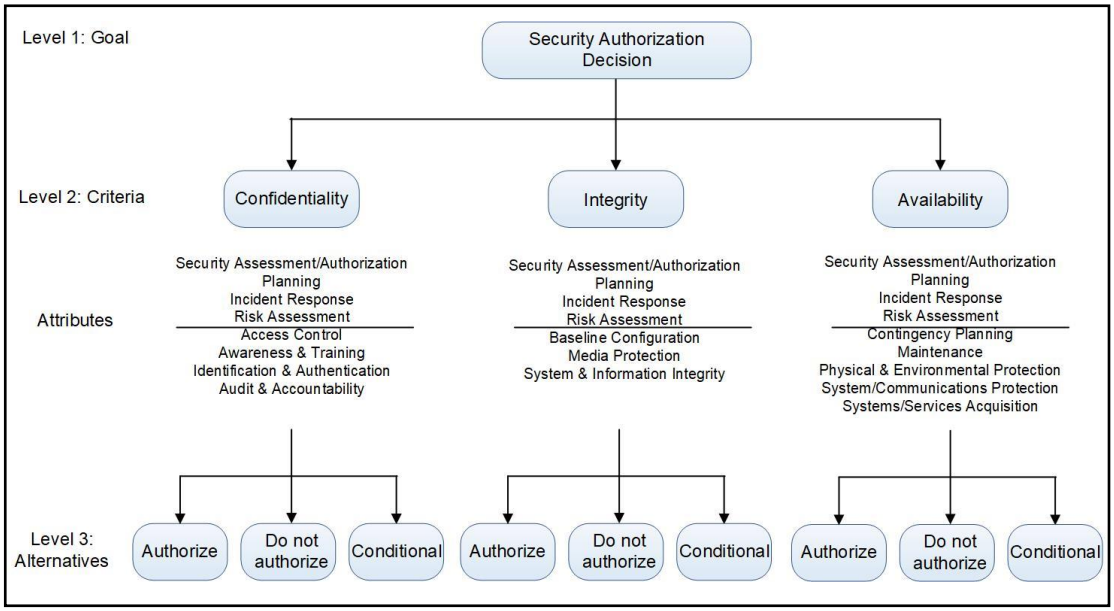

Figure 3-3. Decision Hierarchy

Similar to TOPSIS, the pairwise comparison matrix generated in AHP contains a degree of uncertainty in the relative weights of the decision criteria. The relative weight uncertainty is "caused by the uncertainty in our decision judgements and in many cases cannot be avoided" (Zahir, 1991). Zahir examines uncertainty as independent of judgment consistency and shows how AHP incorporates uncertainty into its computational procedures (Zahir, 1991).

AHP was selected as the most appropriate MCDM method because of its ability to consider a set of evaluation criteria and a set of alternative options from which the best

decision can be made (Saaty, 1980). Another factor in selecting AHP for the security authorization decision-making process is that it is a “fast and understandable method for people who are not familiar with multi-criteria decision support methods.” (Tscheikner-Gratl, 2017). While familiar with the relevant decision criteria, Authorizing Officials will most often have limited, if any, knowledge with multi-criteria decision-making methods.

3.3 Phase 3: Data Collection

Data collection focused on qualitative and quantitative datasets. The collected qualitative and quantitative datasets were used to develop the decision matrix, decision criteria, and decision criteria weights used in the model.

3.3.1 Qualitative Data

The primary source for the qualitative dataset is the DoD Cloud Security Requirements Guide. The qualitative dataset identifies decision criteria and associated attributes used for the Criteria component of the AHP-based model. Criteria used in the model are confidentiality, integrity, and availability (CNSSI No. 1253, 2009).

Figure 3-4 shows the qualitative decision criteria with attributes identified in the DoD SRG. Attribute mapping to decision criteria is described following Figure 3-4.

The qualitative attributes assigned to each decision criteria are taken from the DoD SRG. The qualitative attributes, which are the security controls identified in the SRG, provide a description of the decision criteria characteristics. The seventeen (17) attributes identified in the SRG are mapped to the most appropriate decision criteria used in the praxis model.

Of the seventeen discrete qualitative attributes identified in the SRG, four are applicable to all three decision criteria. The attributes Security Assessment/Authorization,

Planning, Incident Response, and Risk Assessment are appropriate descriptors of each of the three decision criteria. These four attributes are not exclusively appropriate to any one decision criteria.

The qualitative attribute mapping shown in Figure 3-4 is derived from guidance published in numerous CNSS, FedRAMP, and DoD publications addressing cloud security considerations and security authorizations.

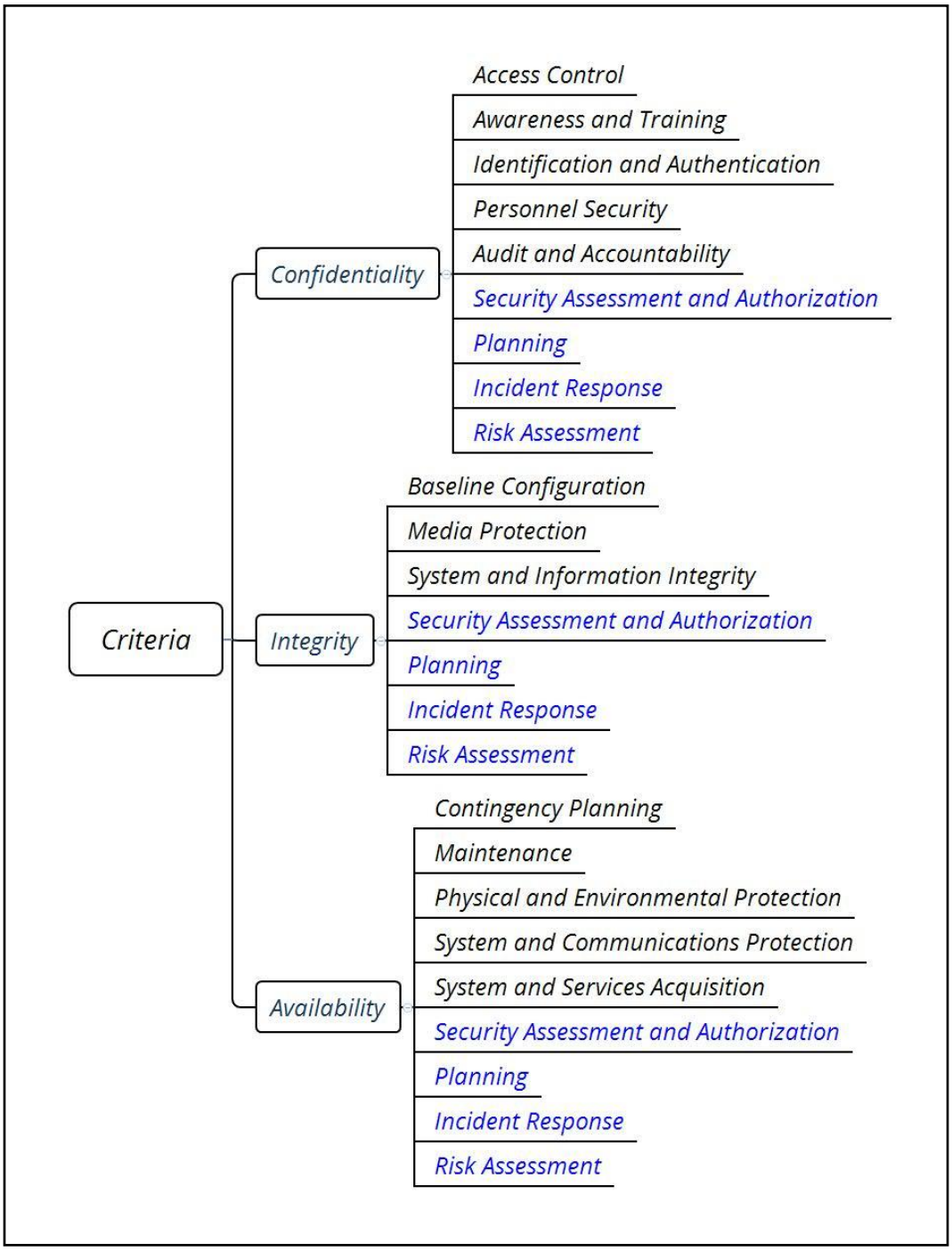

Figure 3-4. Quantitative Decision Criteria with Attributes

3.3.2 Quantitative Data

The quantitative dataset was collected from representative cloud computing security reports published between 2015 and 2018. The quantitative data was used to establish weights and priorities for the three decision criteria. The cloud security reports focus on organizational and decision maker concerns for processing, storing, and securing sensitive data in a cloud computing environment. The security reports covered a total of 3134 respondents from small, medium, and large enterprises.

The Cloud Security Reports used as the quantitative data sources are published annually by Netwrix Corporation and are intended for public consumption. The reports publish the findings from organizations across a range of industries that are asked to identify their security concerns for allowing their organization's sensitive data to be access, stored, or processed by cloud computing technologies. The surveyed organizations are grouped by size according to Gartner's definitions for small, midsize, and large enterprises (Netwrix, 2018).

The respondents whose information is consolidated and published in the annual reports represent technology, manufacturing, government, health care, finance, and education industries. By targeting these industries each year, the reports identify trends and emerging concerns for cloud computing security.

While report results are published in the public domain, the survey questions used to produce the results are proprietary and were not available for inclusion in the praxis. The number of respondents and their industry are available but information such as the percentage of respondents and response success rates are not available from the owner of the report data.

The quantitative data sources are presented in Figure 3-5.

Source	Description
2018 Cloud Security Report Netwrix Corporation	Cloud security report focused on organizational concerns on storing sensitive data in the cloud. 853 respondents 27% from large enterprises (> 1000 employees) 37% from medium buisnesses (100 - 999 employees) 36% from small businesses (1 - 99 employees)
2016 Cloud Security Report Netwrix Corporation	Cloud security report focused on organizational concerns regarding cloud security and readiness to use cloud service offerings. 660 respondents 28% from large enterprises (> 1000 employees) 72% from medium and small businesses
2015 Cloud Security Report Netwrix Corporation	Cloud security report focused on organizational concerns regarding cloud adoption and security. 611 respondents 31% from large enterprises (> 1000 employees) 45% from medium buisnesses (100 - 999 employees) 24% from small businesses (1 - 99 employees)
2015 Cloud Security Spotlight Report Bitglass	Cloud security report focused on organizational adoption of cloud computing and security related concerns and practices. 1010 respondents 40% from large enterprises (> 1000 employees) 42% from medium buisnesses (100 - 999 employees) 17% from small businesses (1 - 99 employees)

Figure 3-5. Quantitative Data Sources

The quantitative data provided by the cloud security reports is mapped to decision criteria attributes used in the model. Mapping the security report data to AHP decision criteria attributes enabled criteria weights to be developed for use in the model. The quantitative data was also used to rank decision alternatives. An analysis of the quantitative data showing how the data was used to establish criteria weights is presented and discussed in Chapter 4.

Figure 3-6 shows the relationship between Phase 3 data collection and Phase 4 data analysis and model refinement.

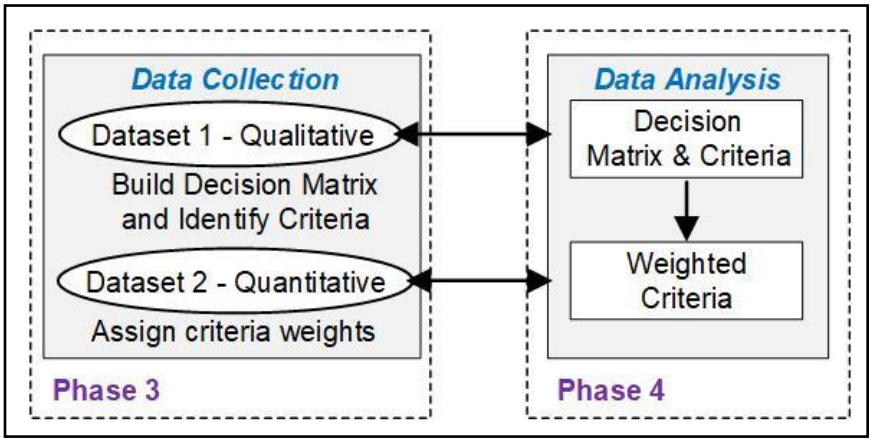

Figure 3-6. Data Collection and Data Analysis Model Phases

3.4 Phase 4: Data Analysis and Model Refinement

During this phase the qualitative and quantitative data collected in Phase 3 was analyzed to refine components and relationships developed in the initial model.

The qualitative data analysis produced the decision matrix, criteria, and attributes associated with the criteria. The AHP Decision Hierarchy developed during this phase is shown in Figure 3-3. The Decision Hierarchy identifies the Goal, Criteria, and Decision Alternatives addressed in the model.

The decision model Goal is the security authorization decision for a cloud service offering. The Criteria upon which the decision is made are confidentiality, integrity, and availability. The alternatives are to authorize the cloud service offering by granting an ATO, not issuing an ATO for the cloud service offering, or granting a conditional ATO with conditions that must be met before an unconditional ATO can be granted.

The quantitative data analysis produced the decision criteria weights and security authorization thresholds.

The decision criteria weights were developed using pairwise comparison and Saaty's Pairwise Comparison Scale (Saaty, 1980). Figure 3-7 shows how, using Saaty's AHP methodology, the criteria weights were calculated and tested for consistency (Saaty, 1980). In the AHP method, the term "consistency" refers to the degree of consistency, or inconsistency, of the decision maker's subjectivity in the pairwise comparison of the importance of decision criteria (Mu, 2017). Consistency of the pairwise comparisons of decision criteria are further discussed in Chapter 4.

3.5 Phase 5: Model Run and Results

After data analysis and refinement of the preliminary model in Phase 4, the AHP model was run using the qualitative and quantitative data analyzed in Phase 4 as input.

The analyzed quantitative security report data was input into the model to calculate decision criteria weights using AHP. Multiple use cases of Saaty's Pairwise Comparison Scale were used to produce candidate selections for mapping verbal judgments to numeric values. The decision criteria weights generated by AHP were tested for consistency using Saaty's Random Index.

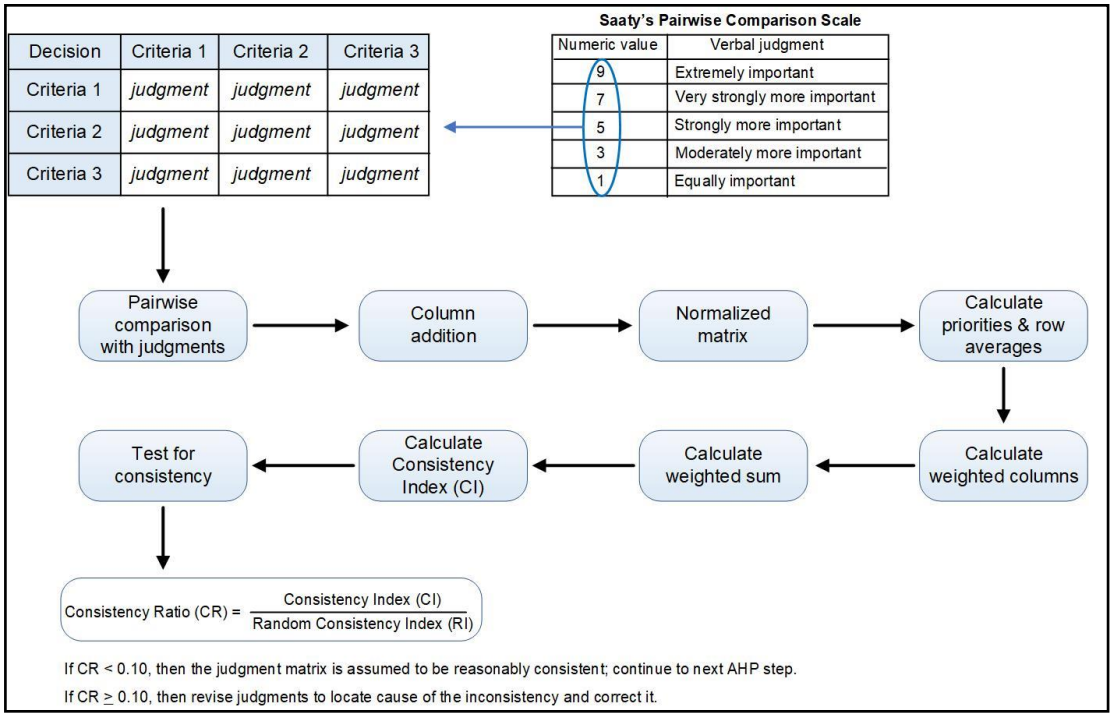

Figure 3-7. Developing AHP Criteria Weights

After the decision criteria weights were calculated and tested for consistency they were applied to the security authorization decision making process to develop a weighted score for several candidate cloud service offerings. The cloud service offerings were rank ordered against each other and against a proposed acceptance threshold (Ø) to help the Authorizing Official make an appropriate security authorization decision.

The detailed steps in the AHP-based model, and the results of running the model using the analyzed qualitative and quantitative data, are presented and discussed in Chapter 4. Chapter 5 discusses the results presented in Chapter 4.

3.6 Phase 6: Validation

The acceptance threshold (Ø) determined by the model is the value below which the mission owner AO will not consider issuing an ATO for a cloud service offering. The acceptance threshold is strongly influenced by the information impact level (IL) and the mission owner's risk tolerance. The Federal Risk and Authorization Management Program (FedRAMP) guides the mission owner in establishing an appropriate IL, risk tolerance position, and approach to security assessments and authorization.

The acceptance threshold (Ø) for issuing a cloud service offering security authorization proposed in the Praxis will be validated by FedRAMP Moderate Controls & Control Enhancement used to guide Federal government cloud computing security authorization decisions. As the number of cloud service offerings that are considered increases, and more data becomes available, the acceptance threshold can be further validated and adjusted as appropriate.

CHAPTER 4 Results

This chapter presents results from running the praxis model. Results are presented for mapping the qualitative and quantitative data sources to decision criteria, AHP decision weight criteria calculations and comparisons, and application of the weighted decision criteria to the security authorization decision making process.

4.1 Security Report Data Analysis Results

The quantitative dataset was collected from representative cloud computing security reports published between 2015 and 2018. The security reports identified in Figure 3-5 provide the quantitative data used to calculate decision criteria weights.

The quantitative data was used to establish weights and priorities for the three decision criteria using Saaty's AHP method (Saaty, 1980). The cloud security reports focus on organizational and decision maker concerns for processing, storing, and securing sensitive data in a cloud computing environment. The cloud security reports cover a total of 3134 respondents from small, medium, and large enterprises across commercial industry and government. The security reports cover the years 2015 to 2018 to reflect how the adoption of cloud computing technology, and associated security concerns, may have changed over time.

The security report data was mapped to decision criteria and criteria attributes. Results of the security report data mapping to decision criteria are shown in Figure 4-1.

Figure 4-1. Mapping Security Report Quantitative Data to Decision Criteria

In Figure 4-1, the data in each of the source security reports was analyzed for relation and relevance to each of the three decision criteria. The percentage of responses in each security report for confidentiality, integrity, and availability security concerns are shown by decision criteria in Figure 4-1.

After the report data was mapped to decision criteria, the data was analyzed to identify the number and percentage of respondents identifying confidentiality, integrity, or availability as one of their security concerns for using cloud computing technology to access, process, or store sensitive data. Results of the analysis were used to establish the relative relationships between the three decision criteria.

Figure 4-2 shows the quantitative data analysis results to include the relationship between the three decision criteria.

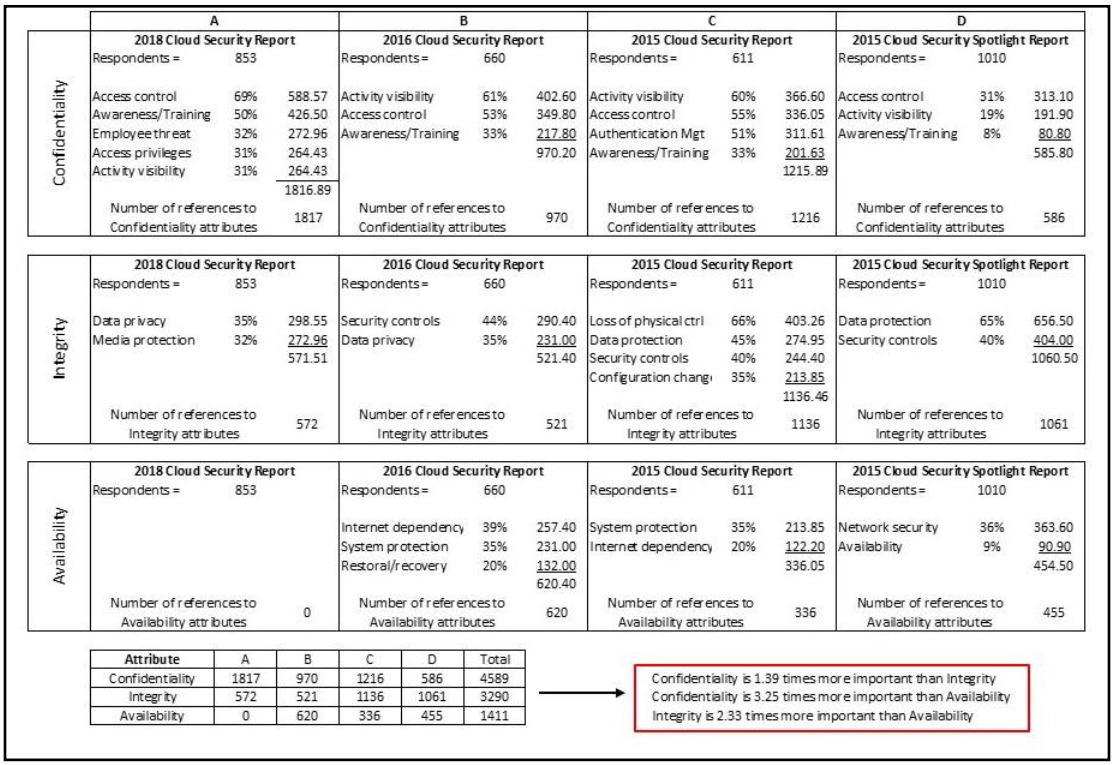

Figure 4-2. Security Report Quantitative Data Analysis

A summary of the data analysis is shown in Figure 4-3.

Figure 4-3 shows the total number of responses indicating security concerns for data confidentiality, integrity, or availability in the four security reports.

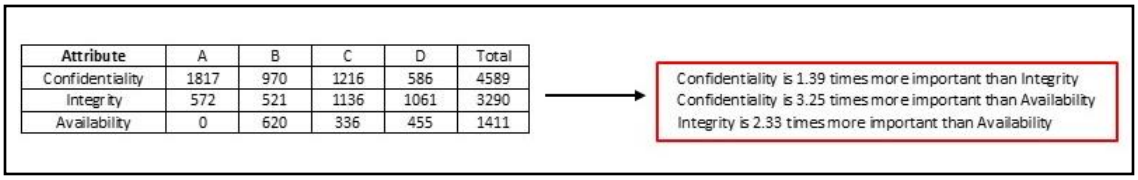

Figure 4-3. Summary of Security Report Quantitative Data Analysis Results

The security report data shows that 4589 responses indicated that confidentiality is a concern for processing or storing sensitive organizational data in a cloud computing environment. Integrity was identified 3290 times and availability was identified 1411 times as security concerns.

The number of responses indicating each of the three decision criteria as security concerns was used to develop the relative relationships between the three decision criteria. The box outlined in red in Figure 4-3 shows that confidentiality is 1.39 times more important than integrity and 3.25 times more important than availability. Integrity is 2.33 times more important than availability for cloud computing security concerns.

The relationships developed from the security report data analysis are used as input to the next step of the AHP process which is to map verbal judgments to numeric values using Saaty's Pairwise Comparison Scale.

4.2 AHP Criteria Weight Calculation

After the security report data analysis was completed, the next step in the model was to calculate decision criteria weights using the quantitative data analysis results. The criteria weights developed by AHP in the praxis replace the equal weights assigned by the DoD Security Requirements Guide to decision criteria in the current security authorization decision-making process. The calculated weights reflect the relative importance of the decision criteria based on the analyzed quantitative data presented in Figure 4-3.

Saaty's Pairwise Comparison Scale was used to translate security report analysis results to numeric values for input into the AHP model. Two use cases were developed using the Numeric Value interpretations shown in Figures 4-4 and 4-5.

Analysis of Survey
Confidentiality is 1.39 times more important than Integrity
Confidentiality is 3.25 times more important than Availability
Integrity is 2.33 times more important than Availability

Saaty's Pairwise Comparison Scale	
Verbal judgment	**Numeric value**
Moderately more important	3
Strongly more important	5
Moderately more important	3

Figure 4-4. AHP Numeric value interpretation; Case 1

Analysis of Survey
Confidentiality is 1.39 times more important than Integrity
Confidentiality is 3.25 times more important than Availability
Integrity is 2.33 times more important than Availability

Saaty's Pairwise Comparison Scale	
Verbal judgment	**Numeric value**
Moderately more important	3
Very strongly more important	7
Strongly more important	5

Figure 4-5. AHP Numeric value interpretation; Case 2

4.2.1 AHP Criteria Weight Calculation; Case 1

The verbal judgment and numeric values used in Case 1 are shown in Figure 4-4. The numeric value is used to calculate criteria weights. For Case 1, the verbal judgments are that confidentiality is moderately more important than integrity, confidentiality is strongly more important than availability, and that integrity is moderately more important than availability. The Numeric Value interpretations used for Case 1 are circled in blue in Figure 4-4.

Tables 4-1 through 4-8 show AHP step-by-step calculations to determine Case 1 criteria weights. Table 4-9 and Table 4-10 show results of criteria weight consistency testing using Saaty's Random Index (RI).

Table 4-1 shows the Case 1 intensity judgments using the Numeric Value assignments shown in Figure 4-4. The highlighted entries in Table 4-1 represent the Numeric Value assignments. As shown in the Confidentiality row, a value of 5 in the Availability column means that Confidentiality is 5 times more important than Availability for the cloud service offering. Likewise, in the Confidentiality row, a value of 3 in the Integrity column means that Confidentiality is 3 times more important than Integrity for the cloud service offering.

Table 4-1. AHP Pairwise Comparison Matrix with intensity judgments; Case 1

Pairwise comparison matrix with intensity judgments

Security Authorization	Confidentiality	Integrity	Availability
Confidentiality	1.000	3.000	5.000
Integrity	0.333	1.000	3.000
Availability	0.200	0.333	1.000

Table 4-2 shows the column addition of the numeric value assignments for each of the three decision criteria. The column sums calculated in Table 4-2 are used to develop the normalized matrix shown in Table 4-3.

Table 4-2. AHP Column Addition; Case 1

Column addition

Security Authorization	Confidentiality	Integrity	Availability
Confidentiality	1.000	3.000	5.000
Integrity	0.333	1.000	3.000
Availability	0.200	0.333	1.000
Sum	1.533	4.333	9.000

Table 4-3 is the normalized matrix for the column additions shown in Table 4-2.

Table 4-3. AHP Normalized Matrix; Case 1

Normalized matrix

Security Authorization	Confidentiality	Integrity	Availability
Confidentiality	0.652	0.692	0.556
Integrity	0.217	0.231	0.333
Availability	0.130	0.077	0.111

Table 4-4 calculates the row averages for each of the decision criteria. The row averages are shown with the original judgments in Table 4-5. The "Priority" column in Table 4-4 represents the weight for each of the decision criteria.

Table 4-4. Calculated priorities with row averages; Case 1

Calculate priorities; row averages

Security Authorization	Confidentiality	Integrity	Availability	Priority
Confidentiality	0.652	0.692	0.556	0.633
Integrity	0.217	0.231	0.333	0.260
Availability	0.130	0.077	0.111	0.106

Table 4-5. Results; Original judgments and priorities; Case 1

Results; original judgments and priorities

Security Authorization	Confidentiality	Integrity	Availability	Priority
Confidentiality	1.000	3.000	5.000	0.633
Integrity	0.333	1.000	3.000	0.260
Availability	0.200	0.333	1.000	0.106

Table 4-6 shows the priorities weights for each criteria and the original judgements shown in Table 4-1.

Table 4-6. Priorities as factors; Case 1

Priorities as factors	Security Authorization	Confidentiality	Integrity	Availability
	Criteria weights	*0.633*	*0.260*	*0.106*
	Confidentiality	1.000	3.000	5.000
	Integrity	0.333	1.000	3.000
	Availability	0.200	0.333	1.000

Table 4-7 shows the weighted column calculations using the weighted criteria and the original judgments.

Table 4-7. Weighted column calculation; Case 1

Calculation of weighted columns	Security Authorization	Confidentiality	Integrity	Availability
	Confidentiality	0.633	0.781	0.531
	Integrity	0.211	0.260	0.318
	Availability	0.127	0.087	0.106

Weighted sum calculations are shown in Table 4-8. The weighted sums calculated in Table 4-8 are used to calculate λ_{max} shown in Table 4-9. λ_{max} is the average of the values calculated in Table 4-8 and is used to calculate the Consistency Ratio of the AHP judgments.

Table 4-8. Weighted sum calculation; Case 1

Calculation of weighted sum	Security Authorization	Confidentiality	Integrity	Availability	Weighted sum
	Confidentiality	0.633	0.781	0.531	1.946
	Integrity	0.211	0.260	0.318	0.790
	Availability	0.127	0.087	0.106	0.320

Table 4-9. λ_{max} calculation; Case 1

Weighted Sum	Priority	
1.945621206	0.633	3.072
0.790082167	0.260	3.033
0.31965812	0.106	3.011
	Total	9.116
Divide total by 3 = λ_{max}		3.039

The next step in the AHP process is to test the judgments using Saaty's Consistency Ratio. The Consistency Ratio (CR) compares the Consistency Index (CI) of the judgment matrix against the consistency index of a random matrix (RI). The random matrix is "one where the judgments have been entered randomly and therefore are expected to be highly inconsistent" (Saaty, 1980). The RI is the average consistency index of 500 randomly filled-in matrices (Saaty, 1980).

Table 4-10 shows the CR calculations for Case 1. In the AHP method, CR = CI/RI. Saaty has shown that a consistency ration of ≤ 0.10 is acceptable to continue with the AHP analysis (Saaty, 1980). A CR of ≤ 0.10 means that the judgments are assumed to be reasonably consistent for application in the AHP method. The RI for n = 3 used in Table 4-10 is 0.58 (Mu, 2017).

Table 4-10. Consistency Ratio calculation; Case 1

	Calculate Consistency Index (CI)	CI = (λmax - *n*) (*n* -1) CI = 0.0194
Test for consistency using Saaty's Random Index (RI)	Consistency Ratio = Consistency Index / Random Index = CI / RI CR = 0.0194 / 0.58 = 0.0334 Acceptance Criteria = CR = CI/RI <0.1	For n=3, RI = 0.58
	CR = 0.0334, the judgment is assumed to be reasonably consistent.	

The consistency ratio calculated for Case 1 = 0.0334 which means that the criteria weight judgments are assume to be reasonably consistent.

4.2.2 AHP Criteria Weight Calculation; Case 2

The verbal judgment and numeric values used in Case 2 are shown in Figure 4-5. Similar to Case 1, the numeric value is used to calculate criteria weights. The Numeric Value interpretations used for Case 2 are circled in blue in Figure 4-5.

Tables 4-11 through 4-18 show AHP step-by-step calculations to determine Case 2 criteria weights. Table 4-19 and Table 4-20 show results of criteria weight consistency testing using Saaty's Random Index (RI).

Table 4-11 shows the Case 2 intensity judgments using the Numeric Value assignments shown in Figure 4-5. The highlighted entries in Table 4-11 represent the Numeric Value assignments. As shown in the Confidentiality row, a value of 7 in the Availability column means that Confidentiality is 7 times more important than Availability for the cloud service offering. Likewise, in the Confidentiality row, a value of 3 in the Integrity column means that Confidentiality is 3 times more important than Integrity for the cloud service offering.

Table 4-11. AHP Pairwise Comparison Matrix with intensity judgments; Case 2

Pairwise comparison matrix with intensity judgments

Security Authorization	Confidentiality	Integrity	Availability
Confidentiality	1.000	3.000	7.000
Integrity	0.333	1.000	5.000
Availability	0.143	0.200	1.000

Table 4-12 shows the column addition of the numeric value assignments for each of the three decision criteria. The column sums calculated in Table 4-12 are used to develop the normalized matrix shown in Table 4-13.

Table 4-12. AHP Column Addition; Case 2

Column addition

Security Authorization	Confidentiality	Integrity	Availability
Confidentiality	1.000	3.000	7.000
Integrity	0.333	1.000	5.000
Availability	0.143	0.200	1.000
Sum	1.476	4.200	13.000

Table 4-13 is the normalized matrix for the column additions shown in Table 4-12.

Table 4-13. AHP Normalized Matrix; Case 2

Normalized matrix

Security Authorization	Confidentiality	Integrity	Availability
Confidentiality	0.677	0.714	0.538
Integrity	0.226	0.238	0.385
Availability	0.097	0.048	0.077

Table 4-14 calculates the row averages for each of the decision criteria. The row averages are shown with the original judgments in Table 4-15. The "Priority" column in Table 4-14 represents the weight for each of the decision criteria.

Table 4-14. Calculated priorities with row averages; Case 2

Calculate priorities; row averages

Security Authorization	Confidentiality	Integrity	Availability	Priority
Confidentiality	0.677	0.714	0.538	0.643
Integrity	0.226	0.238	0.385	0.283
Availability	0.097	0.048	0.077	0.074

Table 4-15. Results; Original judgments and priorities; Case 2

Results; original judgments and priorities

Security Authorization	Confidentiality	Integrity	Availability	Priority
Confidentiality	1.000	3.000	7.000	0.643
Integrity	0.333	1.000	5.000	0.283
Availability	0.143	0.200	1.000	0.074

Table 4-16 shows the priorities weights for each criteria and the original judgements shown in Table 4-11.

Table 4-16. Priorities as factors; Case

Priorities as factors

Security Authorization	Confidentiality	Integrity	Availability
Criteria weights	*0.643*	*0.283*	*0.074*
Confidentiality	1.000	3.000	7.000
Integrity	0.333	1.000	5.000
Availability	0.143	0.200	1.000

Table 4-17 shows the weighted column calculations using the weighted criteria and the original judgments.

Table 4-17. Weighted column calculation; Case 2

Calculation of weighted columns

Security Authorization	Confidentiality	Integrity	Availability
Confidentiality	0.643	0.849	0.516
Integrity	0.214	0.283	0.369
Availability	0.092	0.057	0.074

Weighted sum calculations are shown in Table 4-18. The weighted sums calculated in Table 4-18 are used to calculate λ_{max} shown in Table 4-19. λ_{max} is the average of the values calculated in Table 4-18 and is used to calculate the Consistency Ratio of the AHP judgments for Case 2.

Table 4-18. Weighted sum calculation; Case 2

Calculation of weighted sum

Security Authorization	Confidentiality	Integrity	Availability	Weighted sum
Confidentiality	0.643	0.849	0.516	2.008
Integrity	0.214	0.283	0.369	0.866
Availability	0.092	0.057	0.074	0.222

Table 4-19. λ_{max} calculation; Case 2

Weighted Sum	Priority	
2.0083	0.643	3.121
0.8662	0.283	3.062
0.2223	0.074	3.013
	Total	9.197
Divide total by 3 = λ_{max}		3.066

The next step in the AHP process is to test the judgments using Saaty's Consistency Ratio. The Consistency Ratio (CR) compares the Consistency Index (CI) of the judgment matrix against the consistency index of a random matrix (RI).

Table 4-20 shows the CR calculations for Case 2. In the AHP method, CR = CI/RI. Saaty has shown that a consistency ration of ≤ 0.10 is acceptable to continue with the AHP analysis (Saaty, 1980). A CR of ≤ 0.10 means that the judgments are assumed to be reasonably consistent for application in the AHP method. The RI for n = 3 used in Table 4-10 is 0.58 (Mu, 2017).

Table 4-20. Consistency Ratio calculation; Case 2

	Calculate Consistency Index (CI)	CI = (λmax - *n*) (*n* -1) CI = 0.0328
Test for consistency using Saaty's Random Index (RI)	Consistency Ratio = Consistency Index / Random Index = CI / RI CR = 0.0328 / 0.58 = 0.0565	For n=3, RI = 0.58
	Acceptance Criteria = CR = CI/RI <0.1 **CR = 0.0565, the judgment is assumed to be reasonably consistent.**	

The consistency ratio calculated for Case 2 = 0.0565 which means that the criteria weight judgments are assumed to be reasonably consistent.

4.2.3 AHP Criteria Weight Calculation; Case 1 and Case 2 Comparison

Figure 4-6 shows the Case 1 and Case 2 comparisons for criteria weight calculations and consistency testing. The Consistency Ratio (CR) for both cases is shown in the figure.

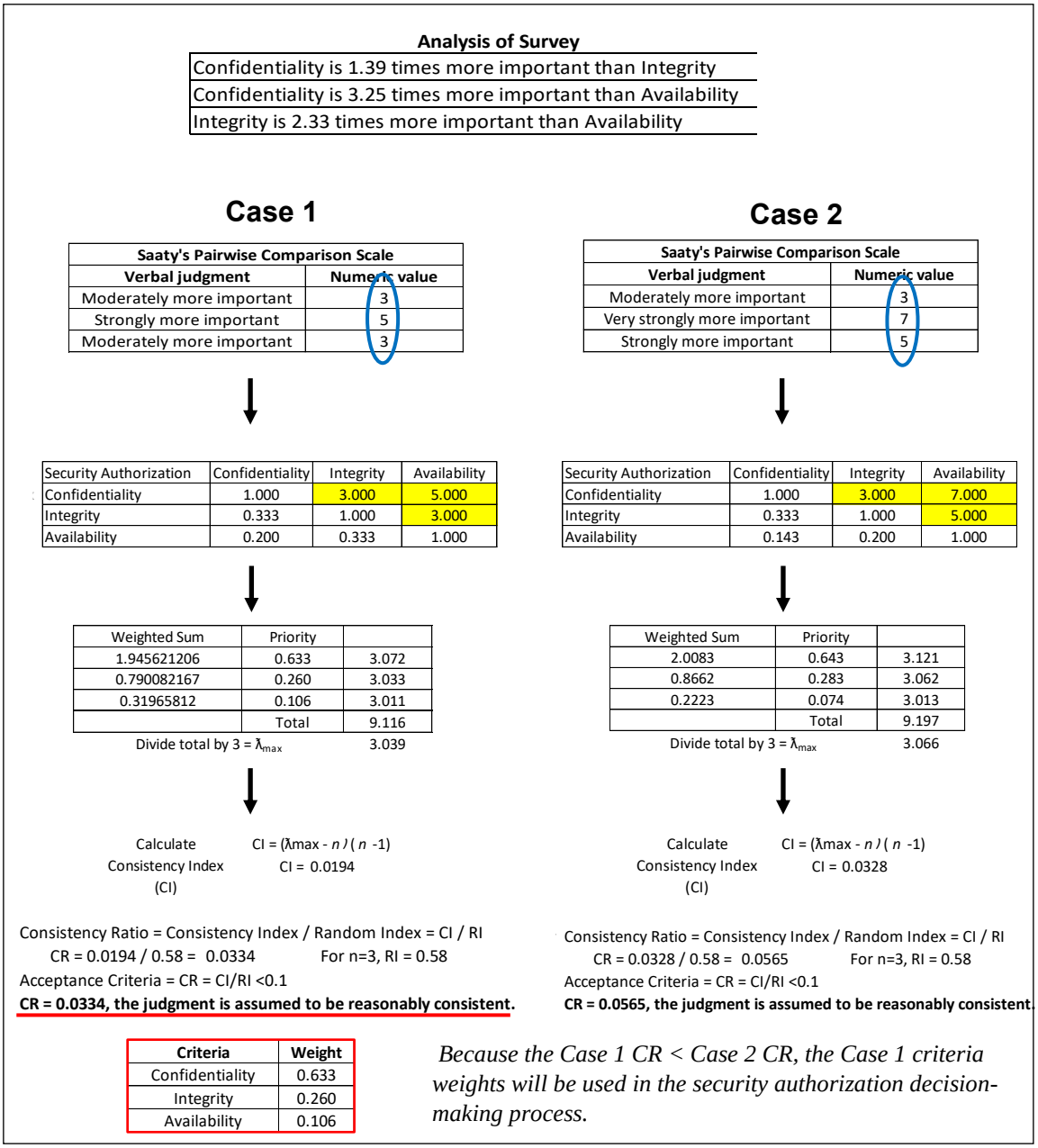

Figure 4-6. Case 1 and Case 2 Comparison

The judgment used in the AHP method is assumed to be reasonably consistent when the CR is determined to be < 0.1. The CR for both cases is in the acceptance range for judgment consistency. Case 1 criteria weighting were chosen for the next step in the model because the Case 1 CR < Case 2 CR indicating that Case 1 judgments are more consistent that Case 2 judgments.

4.3 Applying the Weighted Criteria to the Security Authorization Decision Making Process

The Case 1 criteria weights calculated using AHP were used to develop weighted scores for five cloud service offerings. Table 4-21 shows the criteria, criteria weights, number of attributes against which the cloud service offerings were evaluated, and objective and acceptance threshold values. The values in the Criteria weight column come from Figure 4-6.

Table 4-21. CSO Evaluation Matrix

			O = 1.0	**Ø = .85**
Criteria	**Criteria weight**	**# Attibutes**	Objective (O)	Threshold (Ø)
Confidentiality	0.633	89	89	75
Integrity	0.26	73	73	62
Availability	0.106	81	81	69

The attributes against which the cloud service offerings were evaluated are identified in the DoD Security Requirements Guide. Appendix A shows Security Requirements Guide attributes associated with each of the three decision criteria.

The Objective (O) value represents the ideal situation in which all criteria attributes are satisfied by the cloud service offering.

The Acceptance Threshold (Ø) value is the value below which the mission owner AO will not consider issuing an ATO for the cloud service offering.

The Acceptance Threshold is strongly influenced by two factors. The first factor is the Information Impact Level (IL) of the information that will be processed, hosted, and stored through the cloud service offering. The mission owner determines the appropriate information level.

The second factor is the mission owner's risk tolerance. The risk tolerance is based on the mission owner's assessment of the potential impact if the confidentiality, integrity, or availability of information processed, hosted, or stored through the cloud service offering is compromised.

The Acceptance Threshold proposed in the praxis was developed by using FedRAMP Moderate Controls & Controls Enhancement (C/CE) (FedRAMP SAF, 2017). Of the 116 Moderate C/CE security controls, 99 are recommended for compliance for IL 4 and IL 5 information. Table 4-22 shows the FedRAMP C/CE security controls recommended for the four DoD information levels.

Table 4-22. FedRAMP Moderate Controls & Controls Enhancement (C/CE)

Controls Total	Security Category	Recommended Compliance	Compliance Threshold	Impact Level	Information Type
116	High	113	0.97414	IL6	Classified (SECRET)
116	Moderate	99	0.85345	IL4 and IL5	PII, PHI, FOUO
116	Low	84	0.72414	IL2	Cleared for public release

Five cloud service offerings were run through the model to calculate weighted scores for comparison against each other and against the mission owner's acceptance threshold. Table 4-23 shows the results of the cloud service offering evaluations.

Table 4-23 shows how each of the five CSOs was evaluated against the criteria and associated attributes from the SRG. The criteria weight column is populated with the Case 1 values calculated with the AHP pairwise comparisons and shown in Table 4-5. The Attributes column represents the number of attributes published in the SRG for each criterion.

Table 4-23. CSO Evaluation Results

			CSO 1		CSO 2		CSO 3		CSO 4		CSO 5	
Criteria	**Criteria weight**	**# Attributes**	#	%	#	%	#	%	#	%	#	%
Confidentiality	0.633	89	71	0.798	83	0.933	71	0.798	73	0.820	85	0.955
Integrity	0.26	73	68	0.932	70	0.959	66	0.904	68	0.932	58	0.795
Availability	0.106	81	77	0.951	78	0.963	76	0.938	80	0.988	81	1.000

For each CSO, the number and percentage of attributes that are satisfied by the offering are shown in the "#" and "%" columns respectively. The number and percentage were determined by evaluating the CSO against the Security Requirements Guide for all confidentiality, integrity, and availability attributes.

A weighted score was calculated for each CSO by using the formula shown in Figure 4-7. Detailed calculations for each CSO are shown in Figure 4-8.

Calculate Weighted Scores and Rankings

CSO Weighted Score = (Confidentiality weight)(CSO value) + (Integrity weight)(CSO value) + (Availability weight)(CSO value)

Figure 4-7. Calculating Weighted Scores for a CSO

CSO 1 = (.633)(.798) + (.26)(.932) + (.106)(.951) = 0.84793

CSO 2 = (.633)(.933) + (.26)(.959) + (.106)(.963) = 0.94171

CSO 3 = (.633)(.798) + (.26)(.904) + (.106)(.938) = 0.83950

CSO 4 = (.633)(.820) + (.26)(.932) + (.106)(.988) = 0.86609

CSO 5 = (.633)(.955) + (.26)(.795) + (.106)(1.0) = 0.91713

Figure 4-8. CSO Weighted Scores

After each CSO's weighted score was calculated, the CSOs were rank ordered against each other and also against the mission owner's Acceptance Threshold. Table 4-24 shows the rank order of the five evaluated CSOs. Table 4-25 shows the rank order of the CSOs against each other and against the mission owner's Acceptance Threshold when Ø = 0.85.

Table 4-24. Rank Order of Evaluated CSOs

Alternative	Weighted Score
CSO 1	0.84793
CSO 2	0.94171
CSO 3	0.83950
CSO 4	0.86609
CSO 5	0.91713

Table 4-25. CSO Rankings Against Mission Owner Acceptance Threshold

CSO Ranking		Threshold (Ø) = 85%
Objective	1.00	
CSO 2	0.94171	Above the AO's acceptance threshold; Acceptable.
CSO 5	0.91713	
CSO 4	0.86609	
Threshold	0.85	
CSO 1	0.84793	Below the AO's acceptance threshold; Not acceptable.
CSO 3	0.8395	

Figure 4-9 shows the weighted score for each CSO plotted against the Objective and Threshold values.

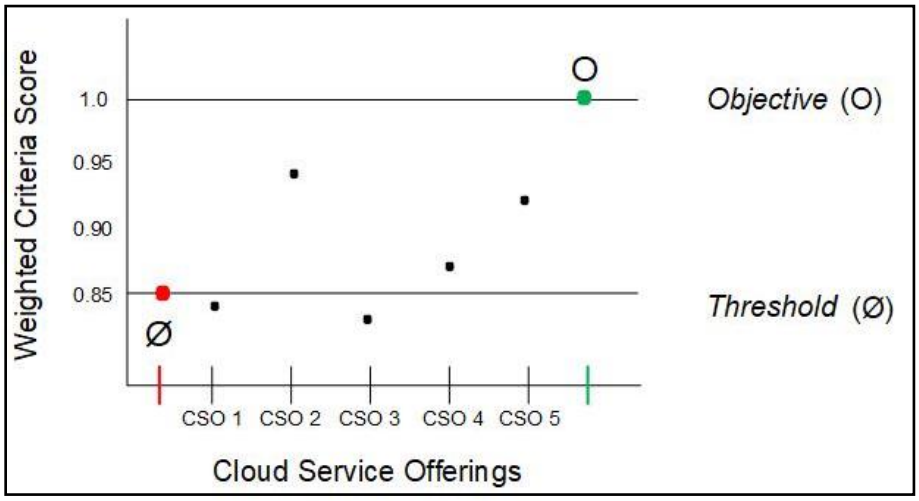

Figure 4-9. CSO Weighted Scores for Ø = 0.85

The weighted scores for CSO 2, CSO 5, and CSO 4 are above the acceptance threshold and these CSOs will be considered for an ATO issued by the mission owner AO when Ø = 0.85. The weighted scores for CSO 1 and CSO3 are below the AO's acceptance threshold so will not be considered for an ATO by the mission owner AO.

The five CSOs were also evaluated with Ø = 0.90 and Ø = 0.95. Results for Ø = 0.90 are shown in Figure 4-10. Results for Ø = 0.95 are shown in Figure 4-11.

CSO Ranking		Threshold (Ø) = 90%
Objective	1.00	
CSO 2	0.94171	Above the AO's acceptance threshold; Acceptable.
CSO 5	0.91713	
Threshold	0.9	
CSO 4	0.86609	Below the AO's acceptance threshold; Not acceptable.
CSO 1	0.84793	
CSO 3	0.8395	

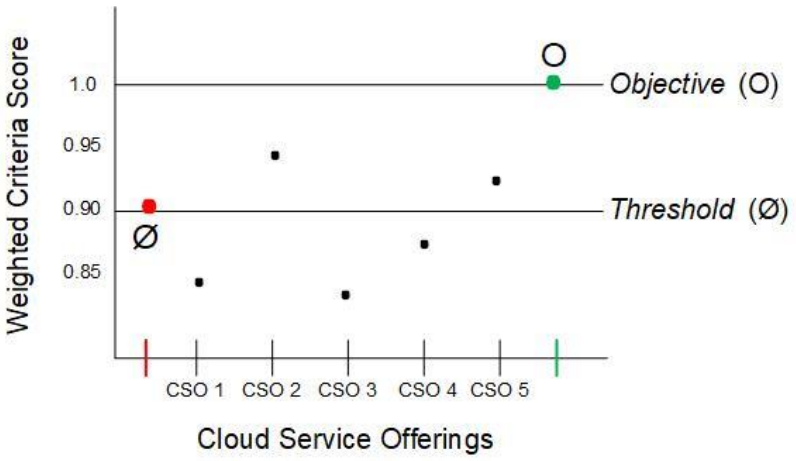

Figure 4-10. CSO Weighted Scores for Ø = 0.90

CSO Ranking		Threshold (Ø) = 95%
Objective	1.00	
Threshold	0.95	
CSO 2	0.94171	Below the AO's acceptance threshold; Not acceptable.
CSO 5	0.91713	
CSO 4	0.86609	
CSO 1	0.84793	
CSO 3	0.8395	

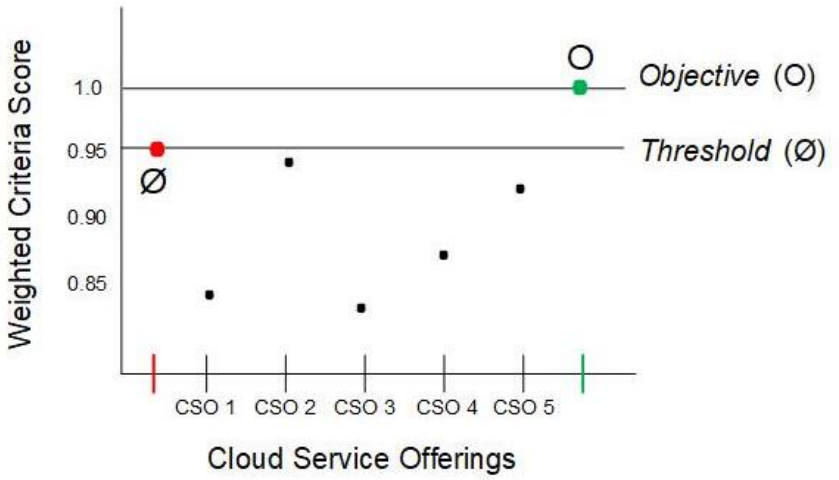

Figure 4-11. CSO Weighted Scores for Ø = 0.95

4.4 Validation

The acceptance threshold (Ø) of 0.85 for issuing a cloud service offering security authorization proposed in the Praxis was validated against current FedRAMP Moderate Controls & Control Enhancement guidance shown in Table 4-22 for Federal government cloud computing security authorization decisions. At Ø = 0.85, three of the five cloud service offerings were assessed as being in the AO's acceptance range.

CSO 2 was selected to host the organization's IL 4 data and applications. For IL 5 data and applications as IL 5, the Authorizing Official may desire a higher Acceptance Threshold based on organizational risk tolerance and the expected impact should the confidentiality, integrity, or availability of the subject data be compromised.

The relatively small number of cloud service offerings that have been granted a security authorization limits the amount of data available for more rigorous validation of the proposed Acceptance Threshold. As the number of cloud service offerings that are subject to security assessments increases, and more data becomes available, the acceptance threshold can be further validated and adjusted as appropriate. The acceptance threshold may be tailored for individual organizations for which the Authorizing Official is responsible for security authorizations.

4.5 Discussion

This section identifies and discusses key findings, hypotheses resolution, and limitations identified from praxis research and model development.

4.5.1 Key Findings

This section discusses key findings from praxis research, model development, and model testing using the weighted criteria and acceptance threshold.

4.5.1.1 Criteria Selection and Weighting

The three criteria used for the security authorization decision are derived from guidance published in the current version of the Security Requirements Guide (SRG). As the SRG, and other relevant DoD cloud computing security guidance, matures additional criteria appropriate for the security authorization decision may be identified.

Criteria weights calculated in the model using the AHP method were based on quantitative data not exclusively from DoD subject matter experts. The quantitative data sources used in the praxis address a wide range of industries, not solely the DoD. The primary reason for including commercial industry concerns for cloud security is because a robust body of quantitative data from DoD subject matter experts does not yet exist. DoD subject matter experts include Authorizing Officials, security engineers, cloud service offering security assessors, and the organizational owners of IL 4 or IL 5 information that is processed or stored in a cloud computing environment.

As cloud computing technology adoption increases within DoD organizations, the body of quantitative data from subject matter experts on DoD-specific security concerns will grow in both volume and depth. The increased amount and depth of quantitative data can be used to refine the weights assigned to the decision criteria.

Of the three decision criteria, availability is most sensitive to the potential uniqueness of the DoD operating environment. The praxis addresses a fixed infrastructure operating environment where connectivity is both robust and reliable. For DoD missions in an austere mobile tactical operating environment, connectivity to cloud resources can be subject to frequent interruption, degradation, high bit error rate channels, and high latency based on environmental challenges. The connectivity challenges inherent to an operating environment solely dependent on satellite communications can make availability significantly outweigh confidentiality and integrity.

4.5.1.2 Determining the Acceptance Threshold

The primary determining factor for the Acceptance Threshold is the mission owner's risk tolerance. Risk tolerance is based on the mission owner's assessment of the

impact if the confidentiality, integrity, or availability of information is compromised. Different mission owners can have different risk tolerances even though they are using similar information.

Attributes such as information perishability and relevance are subjective determinations for which different mission owners may have different interpretations. This subjectivity results in a potentially wide range of acceptance thresholds for authorizing cloud service offerings to connect to DoD networks and access, store, and process information categorized as IL 4 or IL 5. The Acceptance Threshold of 0.85 used in the praxis is based on FedRAMP guidance for assessing the security of cloud service offerings.

The Acceptance Threshold is also influenced by the Information Level of the information which the cloud service offering will access, process, or store. IL 2 information, which is already available in the public domain, can tolerate a lower Acceptance Threshold than IL 4 and IL 5 information. Similarly, classified information categorized as IL 6 will have a higher Acceptance Threshold than the threshold used in this praxis for IL 4 and IL 5 information.

4.5.1.3 Acceptance Threshold Validation

Because a robust body of cloud service offering security assessments for DoD implementations does not yet exist, validation of the proposed Acceptance Threshold is an area for future research. Validation of the 0.85 Acceptance Threshold used in the praxis is based on a limited set of existing cloud service offerings that have been authorized for DoD network connection and information access. As the number of cloud service offerings that are considered increases, the acceptance threshold can be further

validated and adjusted as appropriate. The limited number of currently authorized cloud service offerings for IL 4 and IL 5 does not prevent the praxis model from being applied to the cloud security authorization decision-making process.

The procurement sensitivity of commercial cloud service offering proposals, and the associated DoD security assessment reports, further limits availability of data needed to validate the proposed Acceptance Threshold used in the praxis. Validation of the Acceptance Threshold in the praxis is based on first-hand knowledge of cloud service offerings that have been subject to a security assessment review against SRG security controls for IL4 and IL5 implementations. Because of the procurement sensitivity of cloud service offering proposals and security assessments, it is not possible to access a robust repository of archived data that can be used for acceptance threshold validation.

As the volume of cloud service offering security authorization data grows, validation of proposed Acceptance Thresholds will be based on a more robust collection of historical performance and security data.

4.5.2 Hypothesis Resolution

The null hypothesis ($H1_0$) that applying multi-criteria decision-making methods using weighted decision criteria cannot increase the consistency, repeatability, and objectivity of cloud service offering security authorization decision making was rejected. The AHP multi-criteria decision-making method was applied to calculate and assign weights to decision criteria identified from an analysis of qualitative and quantitative data published in the SRG and the referenced cloud security reports. The weighted decision criteria and Acceptance Threshold developed in the praxis produce a more consistent and repeatable process by removing subjective and equally weighted decision criteria.

4.5.3 Limitations

The two most significant limitations of the praxis research are the limited amount of data available for Acceptance Threshold validation and the procurement sensitive nature of cloud service offerings that can be used as model input and for threshold validation. These limitations provide opportunities for future research.

Section 4.5.1.3 addresses the limited amount of available data that can be used to validate the proposed Acceptance Threshold for issuing a security authorization. As more DoD mission owners perform cloud service offering security assessments and issue security authorizations, validation of the mission owner's Acceptance Threshold will be both more thorough and accurate.

The limitation created by the procurement sensitive nature of cloud service offerings restricts the number of sources that could be used as model inputs. Commercial cloud service providers submit service offering proposals to the DoD that almost always contain proprietary information with very limited authorized distribution terms and conditions. Access to cloud service offerings, and associated security assessment reports, is tightly controlled and limited to procurement officials, proposal evaluators, and security assessors. Because of the restrictive nature of the cloud service offerings and their security assessments, there is not a robust collection of data sources currently available that can be input into the praxis model. The ability to compare multiple cloud service offering security strengths and weaknesses is also limited because of the restrictions on access to the commercial offerings.

4.6 Chapter Summary

This chapter presented results from running the praxis model using the analyzed qualitative and quantitative data. Results were presented for mapping the qualitative and quantitative data sources to decision criteria, AHP decision weight criteria calculations and comparisons, and application of the weighted decision criteria to the security authorization decision making process. Figure 4-12 shows the how model results are applied to the security authorization decision-making process.

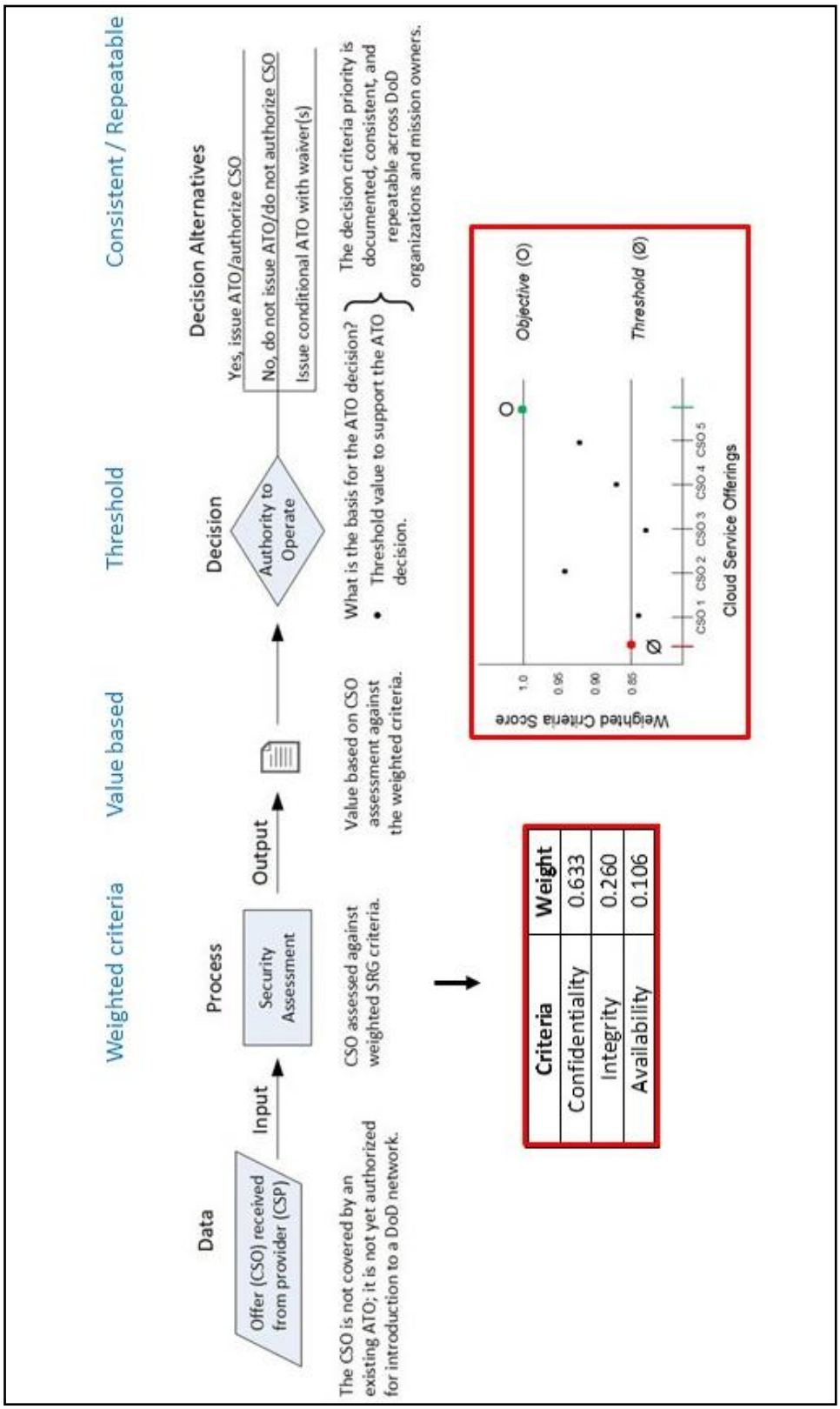

Figure 4-12. Applying Model Results to the Security Authorization Decision-Making Process

CHAPTER 5 Conclusion

The model developed in the praxis successfully met the research objectives and successfully answered the research questions. By applying MCDM methods, the model produced a consistent and repeatable cloud computing security authorization decision-making process.

5.1 Conclusion

Cloud computing offers potential benefits in terms of increased efficiency for information technology (IT) resource utilization along with reduced IT infrastructure procurement and sustainment costs. Along with potential benefits, there are significant security challenges that must be addressed as the DoD aggressively increases its use of cloud computing technology. Confidentiality, integrity, and availability of data hosted in cloud computing environments are critical issue for Government consumers, organizations, and mission owners.

This Praxis produced a decision support model that can be used by DoD security authorizing officials to identify and assess considerations as part of the security authorization decision-making process. The model used Multi-Criteria Decision-Making methods to help mission owners make appropriate security authorization decisions.

The Praxis identified decision criteria, developed criteria weights, and produced a model for evaluating cloud service offerings against the weighted security authorization decision criteria. The model developed in the praxis produces a consistent and repeatable means for making security authorization decisions for cloud service offerings.

5.2 Practical Application

The current lack of common decision criteria and priority of the criteria creates an inconsistent and potentially subjective security authorization decision-making process for DoD cloud service offerings. The praxis research removes inconsistency and subjectivity in DoD cloud security authorization decision-making which results in a reduced level of risk potentially introduced to DoD networks, data, and applications by the authorized cloud service offerings.

The praxis research developed a consistent and repeatable process for DoD Authorizing Officials to conduct security assessments and make security authorization decisions for cloud service offerings. The decision support model developed in the praxis can be immediately and directly applied by DoD Authorizing Officials and security engineers as a component of the cloud security authorization decision-making process.

5.3 Future Research

Future research into cloud service offering security authorizations can focus on three areas. Future research focus areas are:

- Potentially identifying additional decision criteria as part of the model.
- Extending the model's application to classified IL 6 data.
- Analyzing the impact analyzing of the operating environment characteristics on criteria weights

As the Security Requirements Guide continues to mature and updated versions are released, the number of decision criteria may grow beyond the three criteria used in the praxis. Additional security controls and attributes that may be added to future versions of the Security Requirements Guide or applicable FedRAMP guidance can allow

identification of additional decision criteria. Also, cloud computing security concerns common to non-DoD organizations can be researched, identified, and incorporated into the DoD security authorization decision-making process.

Future research can focus on extending the model's application to classified Information Impact Level 6 data. One potential focus area for future research is whether an Acceptance Threshold other than 100% is appropriate for cloud service offerings that will access, process, or store classified information.

For classified IL 6 cloud service offerings, the Objective and Acceptance Thresholds may be the same which prohibits the mission owner AO from granting conditional security authorizations with waivers for specific security controls.

Future research can also focus on analyzing the impact of the operating environment characteristics on criteria weights. For an operating environment where the cloud service offering is accessed through either limited capacity communications channels or channels with high bit error rates and frequent service disruptions, the criteria weights may be impacted. In this challenging operating environment, availability of the cloud resource may gain importance in relation to the confidentiality and integrity of the information.

This is because regardless of how high the level and assurance of information confidentiality and integrity, if the information cannot be accessed when it is needed, the other criteria are potentially significantly reduced in importance.

As cloud computing capabilities are assessed for performance and security suitability in a communications-challenged operating environment, the decision criteria weights for the security authorization decision can change. For current DoD use of cloud computing technologies, availability is provided through robust, resilient, and high-capacity

communications channels. As cloud computing service offerings are considered for use in highly mobile and limited bandwidth environments, the decision model can be adapted to address changing weights for security authorization decision criteria weights.

References

Adriyendi, 2015. *"Multi-Attribute Decision Making Using Simple Additive Weighting and Weighted Product in Food Choice."* International Journal of Information Engineering and Electronic Business, Vol 6, pp. 8-14, 2015.

Agarwal, Ayush, Siddhant Siddharth, and Pratosh Bansal, 2016. *"Evolution of Cloud Computing and Related Security Concerns."* 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, Madhya Pradesh, India, March 18-19, 2016.

Aruna, E., Abirami Shri, and Ajanthaa Lakkshmanan, 2013. *"Security Concerns and Risk at Different Levels in Cloud Computing."* 2013 International Conference on Green Computing, Communications, and Conservation of Energy (ICGCE), Chennai, India, December 12-14, 2013.

Barakovic, Sabina and Jasmina Barakovic Husic, 2016. *"Short and Sweet: Cloud Computing and Its Security."* 2016 XI International Symposium on Telecommunications (BIHTEL), Sarajevo, Bosnia and Herzegovina, October 24-26, 2016.

Bitglass Cloud Security Spotlight Report, 2015. Accessed July 8, 2017. http://www.bitglass.com/BR_Cloud_Security_Report_2015.pdf

Chen, D. and H. Zhao, 2012. *"Data Security and Privacy Protection Issues in Cloud Computing."* 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23 – 25 March 2012.

Cloud Security Alliance (CSA). "Security Guidance for Critical Areas of Focus in Cloud Computing", Version 2.1. Accessed February 6, 2018. http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.

Committee on National Security Systems (CNSS). 2015. CNSS Instruction (CNSSI) No. 4009; Glossary. Ft Meade, MD: April 2015.

Committee on National Security Systems (CNSS). 2009. CNSS Instruction (CNSSI) No. 1253; Security Categorization and Control Selection for National Security Systems, Version 1. Ft Meade, MD: October 2009.

Daniel, Esther, S. Meena, and N.A. Vasanthi, 2013. "*Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions*," 2013 International Conference on Circuits, Power, and Computing Technologies (ICCPCT), Nagercoil, India, March 20-21, 2013.

Elena, Gianfranco, 2015. *"Risk Perception and Cloud Computing Security."* Accessed March 11, 2018. http://www.dcs.gla.ac.uk/~johnson/IFIP13.5/papers/Gianfranco.pdf

Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework (SAF) Version 2.4. 2017. Washington, DC: November 2017.

Federal Risk and Authorization Management Program (FedRAMP) Agency Authorization Roles & Responsibilities for FedRAMP CSPs and Agencies, 2017. Washington, DC: December 2017.

Federal Risk and Authorization Management Program (FedRAMP) Agency Authorization Playbook, 2017. Washington, DC: November 2017.

Figliola, Patricia Moloney, and Eric A. Fischer, 2015. *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal*

Information Technology Reform Management. Washington DC. Congressional Research Service.

Foote, Kenneth E., 2010. *"An Introductory Overview to Multi Criteria Evaluation."* Accessed November 10, 2017. https://www.colorado.edu/geography/foote/2010/Methodology_Norlund_final.ppt.

Gani, Abdullah, Mohammad Nazmul Haque, Nor Badrl Anuar, and Israat Haque, 2014. *"Cloud Service Selection Using Multicriteria Decision Analysis."* The Scientific World Journal, Vol. 2014, Article ID 459375, February 2014.

Gavade, Rohan, 2014. *"Multi-Criteria Decision Making: An Overview of Different Selection Problems and Methods."* International Journal of Computer Science and Information Technologies, Vol. 5(4), pp. 5643-5646, 2014.

Georgiadis, Daniel R., Thomas A. Mazzuchi, and Shahram Sarkani, 2013. *"Using Multi-Criteria Decision Making in Analysis of Alternatives for Selection of Enabling Technology."* Systems Engineering, Vol. 16, No. 3, 2013.

Grobauer, Bernd, Tobias Walloschek, and Elmar Stocker, 2010. *"Understanding Cloud Computing Vulnerabilities."* IEEE Security and Privacy, Vol. 9, Issue 2, 2010.

Halabi, Talal, and Martine Bellaiche, 2017. *"Evaluation and Selection of Cloud Security Services based on Multi-Criteria Analysis MCA."* 2017 Workshop on Computing, Networking, and Communications (CNC), Las Vegas, NV, October 9-11, 2017.

Madhubala, Patil R., 2015. *"Survey on Security Concerns in Cloud Computing."* 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Delhi, India, October 8-10, 2015.

Mocenni, Chiari. The Analytic Hierarchy Process. Accessed June 7, 2018. http://www.dii.unisi.it/~monecci/Note_AHP.pdf.

Mu, Enrique and Milagros Pereyra-Rojas, 2017. *Practical Decision Making.* Washington, DC: Springer International Publishing.

Multi-Criteria Analysis: A Manual. Department of Communities and Local Government. Eland House, Bressenden Place, London, 2009. Accessed October 10, 2017. http://www.communities.gov.uk.

Netwrix Cloud Security Report, 2015. Accessed September 22, 2017. http://www.netwrix.com/netwrix_report_cloud_security_2015.pdf

Netwrix Cloud Security Report, 2016. Accessed September 22, 2017. http://www.netwrix.com/2016_cloud_security_report.pdf

Netwrix Cloud Security Report, 2018. Accessed February 5, 2018. http://www.netwrix.com/2018_cloud_security_report.pdf

Odell, Laura, Ryan Wagner, and Tristan Weir. Institute for Defense Analysis (IDA) Paper P-5287. *Department of Defense Use of Commercial Cloud Computing Capabilities and Services.* Alexandria, Virginia: 2015.

Prakash, Chandan and Surajit Dasgupta, 2016. *"Cloud Computing Security Anaysis: Challenges and Possible Solutions."* International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, March 3-5, 2016.

Saaty, T.L., 1980. *The Analytic Hierarchy Process*. New York, NY: McGraw-Hill.

Teuteberg, Frank and Benedikt Martens, 2012. *"Decision-making in Cloud Computing Environments: A Cost and Risk-Based Approach."* Information Systems Frontiers, September 2012.

Triantaphyllou, B. Shu, S. Neto Sanchez, and T. Ray, 1998. *"Multi-Criteria Decision Making: An Operations Research Approach."* Encyclopedia of Electrical and Electronics Engineering, Vol, 15, pp. 175-186, 1998.

Tscheikner-Gratl, Franz, Patrick Egger, Wolfgang Rauch and Manfred Kleidorfer, 2017. "*Comparison of Multi-Criteria Decision Support Methods for Integrated Rehabilitation Prioritization."* Multidisciplinary Digital Publishing Institute *Water*, January 2017.

U.S. Department of Commerce, National Institute of Standards and Technology. 2015. Special Publication 500-316. Framework for Cloud Usability. Gaithersburg: U.S. Department of Commerce.

U.S. Department of Commerce, National Institute of Standards and Technology. 2011. Special Publication 800-145. The NIST Definition of Cloud Computing. Gaithersburg: U.S. Department of Commerce.

U.S. Department of Defense. 2016. Cloud Computing Security Requirements Guide, Version 1, Release 2. Washington, DC: Department of Defense.

U.S. Department of Defense. 2017. DoD Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT). Washington, DC: Department of Defense, July 2017.

U.S. Department of Defense Chief Information Officer, December 2014. Memorandum for Secretaries of the Military Departments. Subject: Updated Guidance on the

Acquisition and Use of Commercial Cloud Computing Services. Washington, DC: Department of Defense.

U.S. Deputy Secretary of Defense. September 2017. Memorandum for Secretaries of the Military Departments. Subject; Accelerating Enterprise Cloud Adoption. Washington, DC: Department of Defense.

U.S. Government Accountability Office (GAO). April 2016. Report to Congressional Requesters. *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*. Washington, DC: April 2016.

Valesquez, Mark and Patrick T. Hester, 2013. *"An Analysis of Multi-Criteria Decision Making Methods."* International Journal of Operations Research, Vol. 10, No. 2, pp. 56-66, May 2013.

Vaquero, L.M., Rodero-Merino L., Caceres J., and Lindner, M., 2009. "*A Break in the Clouds: Towards a Cloud Definition*.", ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, pp. 50-55, January 2009.

Yoon, K. Paul and Ching-Lai Hwang, 1995. *Multiple Attribute Decision Making: An Introduction*. Thousand Oaks, CA: Sage Publications, Inc.

Zahir, M. Sajjad, 1991. *"Incorporating the Uncertainty of Decision Judgements in the Analytic Hierarchy Process."* European Journal of Operational Research, Vol. 53, Issue 2, pp. 206-216, 1991.

Zoie Radulescu Constanta, Alexandru Balog, Delia Mihaela Radulescu, and Mihail Dumitrache, 2016. *"A Decision Making Framework for Weighting and Ranking Criteria for Cloud Provider Selection."* 20th International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, October 13-15, 2016

Appendix A

Criteria		Attributes	Thresholds			
			100% compliance	95% compliance	90% compliance	85% compliance
Confidentiality Weight = 0.633	Access Control	20	20	19	18	17
	Awareness and Training	5	5	4.75	4.5	4.25
	Identification and Authentication	10	10	9.5	9	8.5
	Personnel Security	9	9	8.55	8.1	7.65
	Audit and Accountability	13	13	12.35	11.7	11.05
	Security Assessment and Authorization	13	13	12.35	11.7	11.05
	Planning	4	4	3.8	3.6	3.4
	Incident Response	10	10	9.5	9	8.5
	Risk Assessment	5	5	4.75	4.5	4.25
		89	89	84.55	80.1	75.65
Integrity Weight = 0.260	Baseline Configuration	17	17	16.15	15.3	14.45
	Media Protection	7	7	6.65	6.3	5.95
	System and Information Integrity	17	17	16.15	15.3	14.45
	Security Assessment and Authorization	13	13	12.35	11.7	11.05
	Planning	4	4	3.8	3.6	3.4
	Incident Response	10	10	9.5	9	8.5
	Risk Assessment	5	5	4.75	4.5	4.25
		73	73	69.35	65.7	62.05
Availability Weight = 0.106	Contingency Planning	9	9	8.55	8.1	7.65
	Maintenance	3	3	2.85	2.7	2.55
	Physical and Environmental Protection	7	7	6.65	6.3	5.95
	System and Communications Protection	17	17	16.15	15.3	14.45
	System and Services Acquisition	13	13	12.35	11.7	11.05
	Security Assessment and Authorization	13	13	12.35	11.7	11.05
	Planning	4	4	3.8	3.6	3.4
	Incident Response	10	10	9.5	9	8.5
	Risk Assessment	5	5	4.75	4.5	4.25
		81	81	76.95	72.9	68.85
		243	243	230.85	218.7	206.55