2012

An Approach For Measuring The Confidentiality Of Data Assured By The Confidentiality Of Information Security Systems In Healthcare Organizations

Shawn Michael Gallaher
University of Central Florida

AN APPROACH FOR MEASURING THE CONFIDENTIALITY OF DATA ASSURED BY THE CONFIDENTIALITY OF INFORMATION SECURITY SYSTEMS IN HEALTHCARE ORGANIZATIONS

by

SHAWN MICHAEL GALLAHER
B.S. Ohio University, 2000
M.S. Ohio University, 2002

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Industrial Engineering and Management Systems
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Summer Term
2012

Major Professors: Ahmad K. Elshennawy
Serge Sala-Diakanda

ABSTRACT

Because of the expansion in health information technology and the continued migration toward digital patient records as a foundation for the delivery of healthcare services, healthcare organizations face significant challenges in their efforts to determine how well they are protecting electronic health information from unauthorized disclosure. The disclosure of one's personal medical information to unauthorized parties or individuals can have broad-reaching and long-term impacts to both healthcare providers and consumers. Although several classes and types of methodologies exist for measuring information security in general, a number of overarching issues have been identified which prevent their adaptation to the problem of measuring the *confidentiality* (the protection from unauthorized disclosure) of electronic information in complex organizational systems.

In this study, a new approach for measuring the confidentiality of electronic information in healthcare-related organizations is developed. By leveraging systemic principles and concepts, an information security system (ISS) for assuring the confidentiality of electronic information in healthcare organizations is synthesized. The ISS is defined as a complex system composed of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule information security safeguards and the people, processes, and technologies that contribute to these safeguards. The *confidentiality* of the ISS – a desired emergent property defined in terms of the systemic interactions which are present – represents the measure of protection from the unauthorized disclosure of electronic information.

An information security model (ISM) that leverages the structure and parametric modeling capabilities of the Systems Modeling Language (SysML) was developed for specifying

an ISS in addition to the contained systemic interactions which are present. Through the use of a parametric solver capability, the complex system of equations which quantify the contained interactions was executed for the purpose of generating a measure of confidentiality using a set of user-provided input values – a process referred to as ISM instantiation.

.

For my beloved parents. I express my most heartfelt appreciation and thanks for your enduring love, support, and wisdom. You have instilled in me the belief that with hard work, any goal can be accomplished.

For my wife and children. No one has been asked to sacrifice more on this journey than you. To my wife Kim, I thank you for your love, support, and encouragement – it always reminds me how blessed I am to share life with you. To my sons, Aidan and Liam – I thank you for inspiring me in the most subtle ways. And to Romi…I thank you for revealing the importance of being "consistently persistent" and of having "persistent consistency".

For all other family and friends who have helped to make my endeavors possible, I express to you sincere thanks for your endless support.

ACKNOWLEDGMENTS

To my advisors, Dr. Serge Sala-Diakanda and Dr. Ahmad Elshennawy, I express sincere gratitude for the guidance and assistance that you have provided during the development of this work. I am most grateful for the patience and flexibility that you have shown in taking on a PhD student with a full-time family and job. I am truly grateful for the opportunity to pursue my research interests.

To my remaining committee members, Dr. Nabeel Yousef, Dr. Waldemar Karwowski, and Dr. Petros Xanthopoulos, I thank you for your valuable contributions to this process. Your feedback and participation have helped to ensure the success of this research.

I would like to express sincere thanks to Doug Wilmarth and Atego for generously allowing the use of software products necessary for completing this research.

I would also like to acknowledge the many individuals who have mentored and advised me throughout my academic and industry endeavors. I am truly grateful to have had your influence along the way.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Research Objective

The objective of this research is to formulate an approach for measuring the confidentiality of electronic information in healthcare-related organizations. In the following introductory chapter, a background on the prevalent issues pertaining to the larger subject of the protection of electronic information is provided, thereby supplying the relevant context around of the objective of this research.

1.2 Background and Problem Statement

An electronic health record is a digital representation of an individual's medical history. It contains information related to existing and previous medical conditions, diagnostics, and treatments. In addition, electronic health records contain personally-identifying information such as social security numbers, demographic characteristics, and account information related to health insurance billing and payment activity. The major perceived benefits of electronically storing patients' personal medical information are 1) reductions in potentially life-threatening medical errors, 2) improvements in the overall delivery of healthcare services, and 3) reductions in the long-run cost of delivering these services.

However, despite these advantages, societal concerns regarding the *confidentiality* of their personal medical information are prevalent and represent a significant barrier to the wide-

spread adoption and acceptance of electronic health records. In the context of personal medical information, the term *privacy* is often used. Privacy is a much broader term than confidentiality, with implications regarding the "freedom" to control how information about oneself is disclosed. Confidentiality is a more precise term for this study, as it is related to the concept of "protecting" information.

The disclosure of one's personal medical information to unauthorized parties or individuals can lead to identity theft and healthcare fraud, with long-term financial impacts on both the patient and healthcare provider. Other concerns regarding confidentiality have broader-reaching implications, such as issues related to the denial of healthcare coverage and employment opportunities based on one's personal medical history or demographic profile (Rindfleisch, 1997). One may also cite less-tangible, but equally significant impacts to individuals such as the negative social stigma that can accompany specific medical conditions or treatments.

Because of the perceived benefits, the U.S. Government supports the development of secure and interoperable electronic health records for most Americans by 2014, in addition to an overarching Nationwide Health Information Network (DHHS, 2006). The more-recent Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 has further incentivized the adoption and use of healthcare information technology and electronic health records. As a result of this expansion in the use of information technology and the migration towards electronic health records as the foundation for healthcare service delivery, it is foreseeable that the personal medical information of individuals will continue to propagate throughout organizations that provide healthcare services. Therefore, it is critical for these

organizations to have a thorough understanding of how "well" they are protecting electronically-stored health information.

A typical approach used by organizations for measuring the protection levels of electronic information in their possession involves determining the degree of compliance with industry-specific *information security standards*. These standards seek to measure the protection level of electronic information from three perspectives:

1) Confidentiality: The protection from unauthorized disclosure of information.
2) Integrity: The protection from unauthorized modification of information.
3) Availability: The protection from loss of information.

One such standard is contained in the Health Insurance Portability and Accountability Act (HIPAA) of 1996 to which covered entities that receive, maintain, or transmit personal health information must comply, according to United States Federal law. The HIPAA Security Rule defines a set of administrative, physical, and technical *safeguards* for protecting the confidentiality, integrity, and availability of electronic protected health information (EPHI) (DHHS, 2003). Safeguards consist of mechanisms including 1) policies for controlling access to information resources, 2) software for enforcing and controlling these policies, and 3) physical protection of computing resources. Their primary purpose is to secure the overall information technology and processing *environment* of an organization by protecting information from a well-known range of threats (i.e. conditions or events that adversely impact organizational mission via a compromise of electronic information). However, there are several shortcomings associated with the aforementioned standards:

1) Although an organization may be considered "compliant", there is currently no standard method to delineate how well the organization is performing in each of the three protection perspectives: confidentiality, integrity and availability.
2) The lack of standard methods for delineation, as indicated above, underlines the deeper problem of measurements. Indeed, current information security standards give no indication as to how organizational components such as people, processes, and technology contribute to a specific protection perspective.
3) They do not account for the complex and dynamic nature of information security components.

It results from these observations that information security standards, while recognizing the importance of the confidentiality, integrity and availability of electronic information, lack clear, robust and industry-cutting methodologies for measuring them.

1.3 Systemic Perspective on Information Security

As stated in Section 1.1, the objective of this research is to formulate an approach for measuring the confidentiality of electronic information in healthcare-related organizations. In this research, a *systemic* perspective on information security and confidentiality is adopted. By leveraging systemic principles and concepts, an information security system (ISS) for assuring the confidentiality of electronic information in healthcare organizations is synthesized. The ISS is defined as a complex system composed of the HIPAA Security Rule safeguards and the people, processes, and technologies that contribute to these safeguards. The *confidentiality* of the

ISS - a desired emergent property defined in terms of the systemic interactions which are present - represents the measure of protection from the unauthorized disclosure of electronic information.

In the context of healthcare, this systemic perspective is in line with the Institute of Medicine's vision for healthcare in the 21st century, which identifies not only electronic health records as part of the information infrastructure, but also a systems approach for the practice of healthcare, in which teams of people, processes, and technology interact to achieve desired performance (Stead, 2009). This research addresses the lack of systemic approaches for understanding issues and requirements in the field of information security identified by Hessami and Karcanias (2009), as well as the lack of research related to information security measurement within the healthcare industry identified in the work of Appari and Johnson (2010).

1.4 Document Outline

The remainder of this document is structured in the following manner: Chapter 2 provides an overview of healthcare information security standards and safeguards, reviews the state of information security measurement, and presents the common, standard, and experimental approaches available for measuring information security. In Chapter 3, an approach for measuring the confidentiality of electronic information is developed which consists of synthesizing an ISS, and defining confidentiality as an emergent property of this system. In Chapter 4, an information security model (ISM) is developed for demonstrating the solution developed in Chapter 3. Chapter 5 discusses ISM instantiation, the process by which the ISM is

used for generating a quantitative measure of confidentiality, and provides the corresponding results and analysis. Chapter 6 highlights the significance and contributions of this research to the field of information security, and additionally proposes extensions of this research and directions for future work.

CHAPTER 2

LITERATURE REVIEW

The objective of this chapter is to provide an introduction to healthcare information security standards and information security measurement. Specifically, an overview of healthcare-specific information security standards and safeguards is provided in order to define relevant industry requirements, the general state of information security measurement is discussed, and the major types of methodologies available for measuring information security are reviewed.

2.1 Healthcare Information Security Standards and Safeguards

Modern organizations are required to demonstrate compliance with industry-specific information security standards that are promulgated by overarching laws and regulatory requirements. With respect to healthcare, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 remains the industries principle legislative mechanism regarding information security. Although HIPAA was primarily established to address a broad array of healthcare-related reforms, such as the creation of United States Federal Laws related to the access and portability of healthcare, HIPAA required the Department of Health and Human Services (DHHS) to establish standards for the protection of patient information utilized in the delivery of healthcare services. As such, under the HIPAA Title II Administrative Simplification,

the Privacy Rule and Security Rule were established to address the protection of patient health information. Figure 2-1 provides an illustration of the HIPAA components.

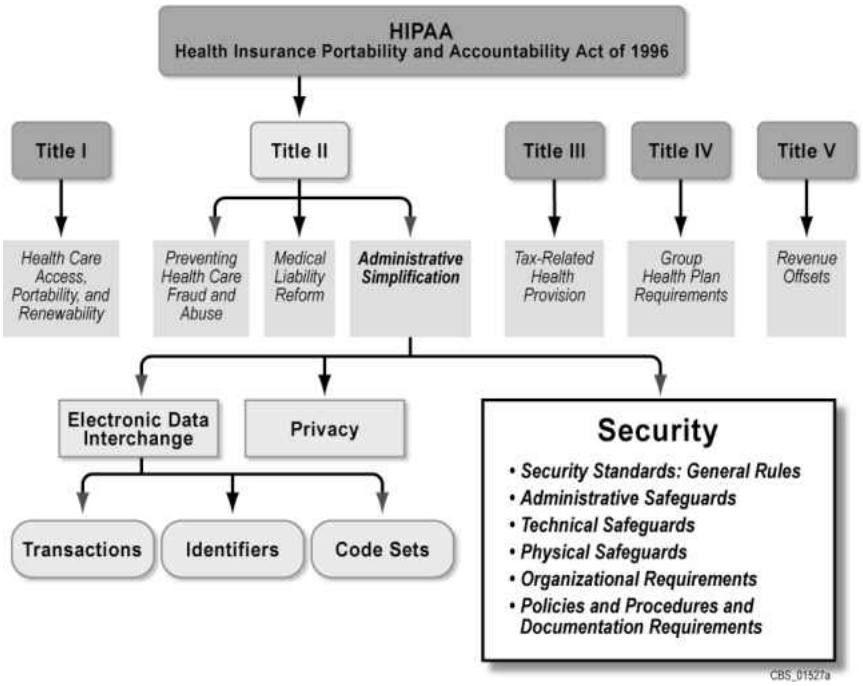


Figure 2-1 HIPAA Components (NIST, 2008)

The HIPAA Privacy Rule, briefly introduced here to clearly distinguish the broadness of its provisions relative to the more-specific focus of the Security Rule, consists of overarching protections that govern the disclosure of Protected Health Information (PHI). PHI consists of information such as an individual's medical status and treatment history, in addition to account information related to health insurance billing and payment activity. The HIPAA Privacy Rule is broad in nature, and PHI can be interpreted as germane to the disclosure health information in *all*

forms, including paper-based documents that contain personal medical information or verbal transmissions in which one's medical information is discussed.

The HIPAA Security Rule is much more specific and directly addresses the protection of electronically-stored PHI, referred to as Electronic Protected Health Information (EPHI). EPHI is a subset of PHI consisting of health information which exists in a *digital* format. The HIPAA Security Rule establishes information security standards and safeguards for protecting the confidentiality, integrity, and availability of EPHI that is received, maintained, or transmitted by organizations. Before introducing the specific safeguards identified in the HIPAA Security Rule, a brief discussion regarding general safeguard concepts is provided.

2.1.1 Safeguard Concepts

Safeguards are the primary mechanisms used for securing the overall information technology and processing environment within an organization. They are intended to protect information from a well-known range of threats (i.e. conditions or events that adversely impact organizational mission via a compromise of information) through the implementation of entity-wide processes, procedures, and other broad protection mechanisms. Examples of safeguards are 1) policies for controlling access to information resources, 2) software for enforcing and controlling the restrictions established by these policies and 3) physical protection of computing resources.

The fundamental concept surrounding safeguards is that they reduce the likelihood of threat-vulnerability exploitation. For example, a procedure for processing separated employees is an example of a typical safeguard present in many information security standards. One of the

primary purposes of this safeguard is to ensure that when an employee separates from an organization, their physical and logical accesses (e.g. badges and information system user accounts) are no longer active. This reduces the likelihood that the separated employee will be able to access information and resources after they are no longer authorized to do so. Figure 2-2 provides an illustration of this scenario, in which the separated employee is the *threat*, their active information system user account is the *vulnerability*, and the procedure for removing an employee's information system access is the *safeguard*.

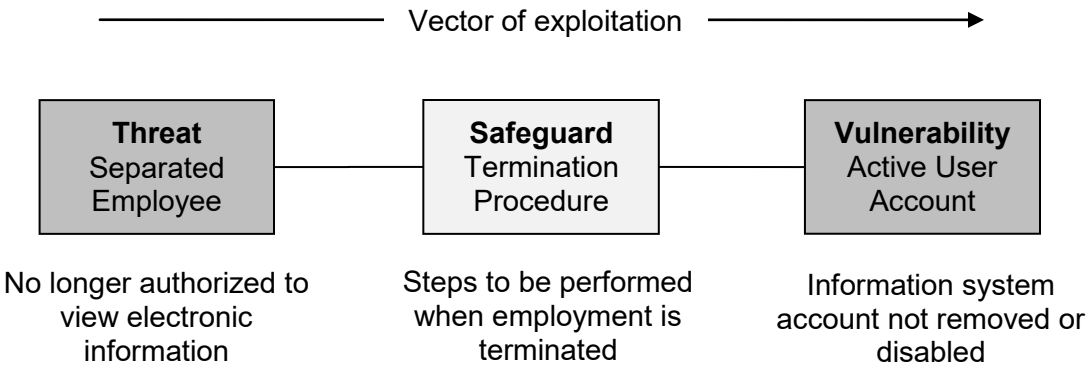


Figure 2-2 Threat-safeguard-vulnerability example

Safeguards exist throughout an organization and are intended to establish the organization's enterprise-wide approach for protecting the electronic information that it maintains. This point is emphasized to establish a clear distinction between safeguards and the individual mechanisms (i.e. configuration settings) that exist within a software application, referred to as application-level controls. Examples of these mechanisms are software-level policy restrictions and validation of user input fields. For example, an EHR software application may

contain application-level controls for validating user input fields that hold data such as a patient's social security number or date of birth to ensure the provided values are correctly formatted or that they exist in a remote database. Other examples of application-level controls include network connectivity settings and detailed interface checks (e.g. control totals and hash checks) for transaction processing. Figure 2-3 illustrates the relationship of safeguards and application-level controls within the organizational environment.

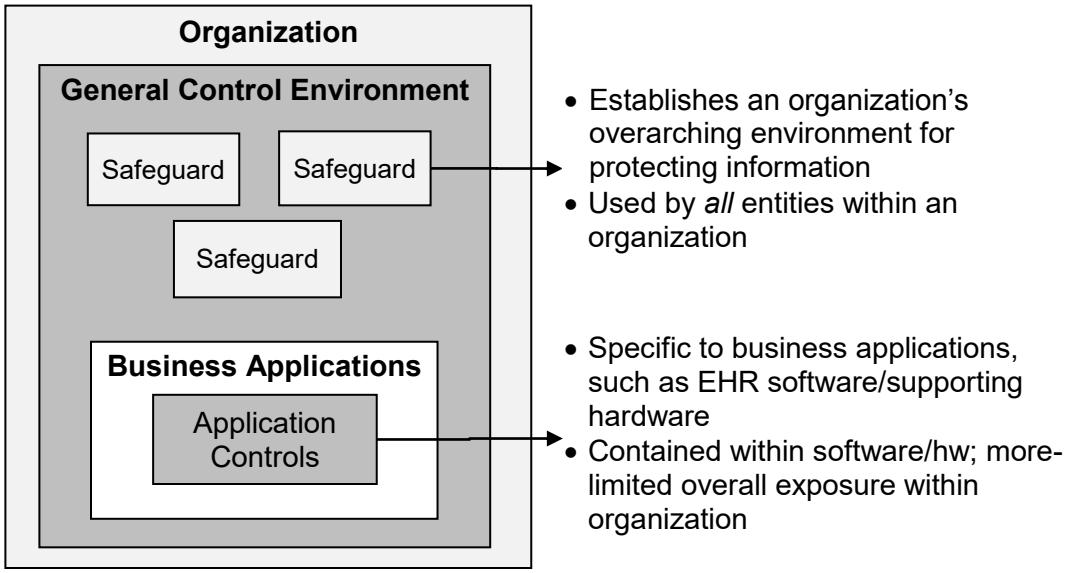


Figure 2-3 Context of safeguards and application controls

Safeguards establish the *general control environment* within an organization because they are applicable to the organization as a whole. The general control environment can be thought of as a conceptual protection space which surrounds lower level business applications, such as EHR processing applications.

While the importance of application-level controls is recognized in the context of total information security, without effective general controls, application controls may be rendered ineffective by circumvention or modification (GAO, 2009). This underscores the generally-accepted notion that even *strong* application controls are more-easily compromised by *weak* safeguards. This point is made to clearly delineate the scope of this research as it relates to the specific concerns regarding the measurement of confidentiality in an organizational context.

2.1.2 HIPAA Security Rule Safeguards

The HIPAA Security Rule defines three types of safeguards for protecting EPHI: *administrative*, *physical*, and *technical*. Each safeguard type consists of individual protection mechanisms intended to protect the confidentiality, integrity, and availability of electronic information within an organization.

The safeguards and corresponding information security standards identified in the HIPAA Security Rule are listed Table 2-1 (Health Insurance Reform: Security Standards; Final Rule, 2003).

Table 2-1 Safeguards defined in the HIPAA Security Rule (HHS, 2003)

Type	Standards	Safeguards
Administrative	▪ Security Management Process ▪ Assigned Security Responsibility ▪ Workforce Security ▪ Information Access Management ▪ Security Awareness and Training ▪ Security Incident Procedures ▪ Contingency Plan ▪ Evaluation ▪ Business Associate Contracts and Other Arrangement	▪ Risk Analysis ▪ Risk Management ▪ Sanction Policy ▪ Information System Activity Review ▪ Authorization and/or Supervision ▪ Workforce Clearance Procedure ▪ Termination Procedures ▪ Isolating Health care Clearinghouse Function ▪ Access Authorization ▪ Access Establishment and Modification ▪ Security Reminders ▪ Protection from Malicious Software ▪ Log-in Monitoring ▪ Password Management ▪ Response and Reporting ▪ Data Backup Plan ▪ Disaster Recovery Plan ▪ Emergency Mode Operation Plan ▪ Testing and Revision Procedure ▪ Applications and Data Criticality Analysis ▪ Written Contract or Other Arrangement
Physical	▪ Facility Access Controls ▪ Workstation Use ▪ Workstation Security ▪ Device and Media Controls	▪ Contingency Operations ▪ Facility Security Plan ▪ Access Control and Validation Procedures ▪ Maintenance Records ▪ Disposal ▪ Media Re-use ▪ Accountability ▪ Data Backup and Storage
Technical	▪ Access Control ▪ Audit Controls ▪ Integrity ▪ Person or Entity Authentication ▪ Transmission Security	▪ Unique User Identification ▪ Emergency Access Procedure ▪ Automatic Logoff ▪ Encryption and Decryption ▪ Mechanism to Authenticate Electronic Protected Health Information ▪ Integrity Controls ▪ Encryption

2.1.3 Primary Issues

Healthcare information security standards and safeguards are beneficial in that they establish baseline protection mechanisms which must be implemented by organizations for adequately protecting electronic information. However, they lack the complement of a standard approach or mechanism for measuring how well the required safeguards are maintaining any specific information security perspective, such as confidentiality. This is a significant shortcoming, as organizations are left to decide how they are meeting these standards and subsequently are left to develop corresponding measurements of confidentiality. It will be shown throughout the remainder of this chapter that, although several general classes of approaches exist for measuring information security in general, a number of overarching issues exist which prevent their adaptation to the problem of measuring confidentiality in complex organizational systems.

The next section provides an overview of the state of information security measurement and discusses how the topic of measurement has been specifically addressed in the literature, both from a general perspective and with respect to healthcare.

2.2 State of Information Security Measurement

National Institute of Standards and Technology Internal Report (NIST-IR) 7564 "Directions in Security Metrics Research" states that most formal approaches for security measurement and assessment have achieved only limited success (NIST, 2010). The lack of success with respect to measurement approaches is underscored in the United States Department of Homeland Security (DHS) 2009 Roadmap for Cyber Security Research which identifies the need for enterprise-level security metrics as one of the eleven hard problems facing information security research today (DHS, 2009). DHS and the Information Security (INFOSEC) Research Council, an organization consisting of program managers that sponsor information security research within the U.S. Federal Government, conclude that a lack of universally agreed-upon methodologies for addressing the issue of systems security quantification represents a major gap in information security research.

Specifically within the healthcare industry, there is an observable lack of research regarding information security measurement and metrics. Of the 110 different research papers surveyed by Appari and Johnson in their recent work entitled "Information Security and Privacy in Healthcare: Current State of Research" (2010), only ten (10) are classified by the authors as being related to the *measurement* of healthcare information security and privacy. Table 2-2 provides a summary of these papers.

Table 2-2 Research related to healthcare information security and privacy measurement (Appari and Johnson, 2010)

Author	Year	Title
Cheng, Hung	2006	Towards a Privacy Access Control Model for e-Healthcare Services
Choudhury, Ray	2007	Privacy Management in consumer e-Health
Dong, Dulay	2006	Privacy Preserving Trust Negotiation for Pervasive Healthcare
Ball, Gold	2007	Banking on health: personal records and information exchange
Hu, Ferraiolo, Kuhn	2006	Assessment of Access Control Systems
Truta, Fotouhi. Barth-Jones	2004	Disclosure Risk Measures for the Sampling Disclosure Control Method
Truta, Fotouhi, Barth-Jones	2004	Assessing Global Disclosure Risk in Masked Microdata
Truta, Fotouhi, Barth-Jones	2003	Disclosure Risk Measures for Microdata
Truta, Fotouhi ,Barth-Jones	2003	Privacy and Confidentiality Management for the Microaggregation Disclosure Control Method: Disclosure Risk and Information Loss Measures
Winkler	2004	Masking and Re-identification Methods for Public-Use Microdata: Overview and Research Problems

A review of the publications listed in Table 2-2 indicates that they are related to the masking of electronic data, or provide technical solutions related to the design of access control mechanisms. While related to the confidentiality of electronic information, they are more focused on the technical aspects of information protection. A focus on the purely technical aspects of information security is an overarching characteristic associated with the existing body of information security research (Oinas-Kukkonen and Siponen, 2007). Unfortunately, these types of approaches, although valuable contributions, do not offer solutions that organizations can use for measuring confidentiality in an enterprise context. The lack of organizational-level approaches for information security measurement in healthcare is critical, given that it is now

well understood that information security is no longer limited to any single technical aspect, but is in fact germane to an organization as a whole (Dhillon and Backhouse, 2000).

The remainder of this chapter reviews common, standard, and experimental approaches that are available for measuring information security. This will provide an overview of existing approaches and their suitability for adaptation to the problem as stated in Chapter 1. In addition, a summary of the underlying issues and gaps associated with existing approaches is provided. Figure 2-4 summarizes the information security measurement approaches reviewed in this section.

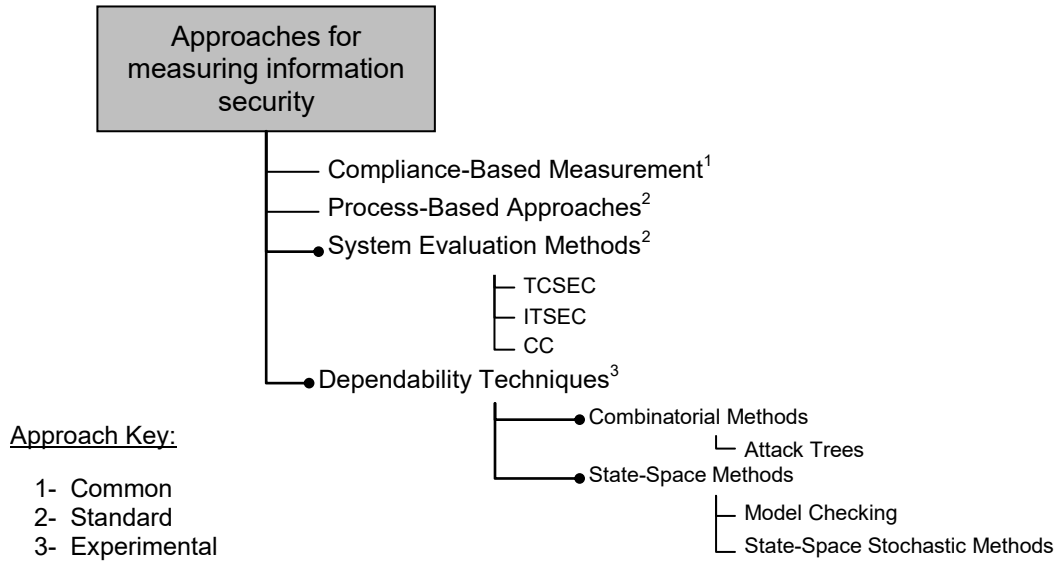


Figure 2-4 Approaches for information security measurement

2.3 Compliance-Based Measurement

One of the most-common and generally-accepted practices within organizations is to derive measurements of information security from assessments of compliance with information security standards. The general approach involves the following steps: (1) construct a list of required safeguards using compliance standards, (2) determine if the safeguards have been implemented, (3) make a determination regarding the effectiveness of *each* safeguard, if it has been implemented, (4) and make a final determination regarding the overall level of compliance. Figure 2-5 illustrates the basic flow of the compliance-based measurement process.

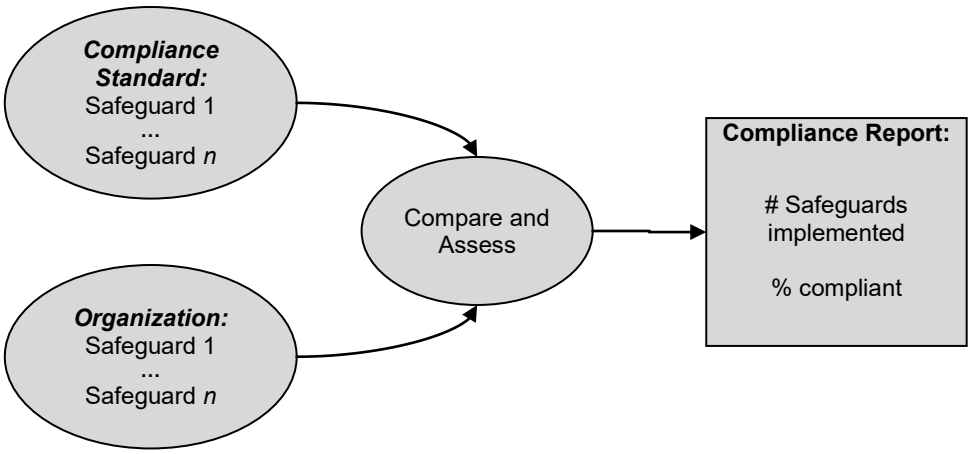


Figure 2-5 Basic flow of compliance-based measurement of information security

Compliance-based assessments are beneficial in that they provide a broad perspective from which organizations can begin to evaluate their approach to information security. In addition, they are advantageous in that they can be used for demonstrating progress toward

compliance with industry-specific laws regarding information protection. This is a critical concept for organizations, particular those related to healthcare, in which favorable progress can assist in fostering public trust regarding the protection of personal medical information.

A primary concern with measures of information security generated using compliance-based approaches is that they are typically procedural and subjective in nature (DHS, 2009). The resulting metrics for information security consist of values such as "percentage of mandatory safeguards implemented" or the "number of systems reviewed". More specifically, there is no standard or generally accepted practice for what exists within the "compare and assess" component shown in Figure 2-5.

Hulitt and Vaughn (2008) propose a quantitative measure of compliance based on Pathfinder Networks. The authors show that a quantitative network representation can be generated of the proximity data of threat-vulnerability pairs in an open-risk model and Federal Information Security Management Act (FISMA) compliant model of information system safeguards. The result is a "% compliant" metric indicating the percentage of safeguards implemented. Their approach is novel in that overcomes the qualitative limitation of compliance standards. However, although it provides a good measure of information security with respect to compliance, it is limited by the fidelity of the standard that it uses for comparison. As a result, it does not provide individual indicators regarding specific types of protection based on the set of safeguards.

2.3.1 Underlying Issues

Because information security standards typically treat information security as a generic concept, organizations are left to determine how the various safeguards contribute to each type of protection, such as confidentiality. As a result, it is difficult to determine the level of any single type of protection provided by a set of safeguards. This is problematic when organizations attempt to determine where resources should be applied to address industry-specific concerns, such as confidentiality in the case of healthcare organizations.

Compliance-based approaches also lack the foundation of an underlying model on which measurements can be based. As noted by Wang (2005), the absence of an underlying model is a common issue associated with measurements of information security. For example, although the safeguards shown in Table 2-1 are broadly classified as administrative, physical, and technical, there is no model that places them in the context of the supporting organizational components (i.e. people, processes, and technology). In addition, in the practice of assessing information security it is often the case that safeguards are assessed and related measurements are taken in *isolation* as opposed to in the context of a *system or network of protection*.

Leveraging the example provided in Figure 2-2, it is evident that the effectiveness of termination procedures is impacted by the manner in which information system accounts are established. If a user's access is not formally approved, authorized, and documented, it is less likely that security personnel will know to remove it upon employee separation. Subsequently, the account would remain active until detected via another safeguard that addresses the monitoring and review of information system accounts. Viewing safeguards in an isolated fashion does not account for these types of interactions and as a result measurements of

information security are not truly reflective an organization's ability to maintain the confidentiality of electronic information. The lack of a foundational model is a primary reason for the inability of information security measurement approaches to consistently capture these interactions as part of the measurements and metrics that they produce.

Although it is generally assumed that safeguards apply exclusively to computer and information systems, a growing body of research indicates that issues surrounding information security are not limited to technology, but are germane to the organization as a whole (Dhillon and Backhouse, 2000). Beznosov, Hawke, and Werlinger (2008) discuss the existence of multiple *factors* (e.g. human and technical) that introduce challenges to organizations in their efforts to address information security. Kraemer, Carayon, and Clem (2009) conclude that the interactions of multiple factors contribute to computer and information security *vulnerabilities*. These types of factors are not considered in current information security standards and organizations are left to determine the context in which safeguards are viewed.

The information security-related legislation and standards associated with other industries and domains share the same shortcomings as those presented by the HIPAA Security Rule. For example, the FISMA consists of overarching legislation which requires agencies of the U.S. Federal Government to implement an entity-wide information security program based on the standards and safeguards documented in the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*. NIST SP 800-53 identifies management, technical, and operational safeguards for protecting the confidentiality, integrity, and availability of electronic information (NIST, 2009). NIST has provided guidance regarding how healthcare organizations can

implement the HIPAA Security Rule using the same framework suggested for FISMA and NIST 800-53 implementation (NIST 2008). However, like the HIPAA Security Rule, there is no indication of how the different types of safeguards contribute to each type of protection, nor is there the benefit of an underlying model that addresses safeguard-to-safeguard interactions or their requisite organizational contributors.

2.4 System Evaluation Methods

In this section, system evaluation concepts are reviewed, the primary system evaluation methodologies are described, and their capacity for measuring confidentiality is addressed.

System evaluation methods are used to determine if a target information technology product or system satisfies some set of requirements for security *functionality* and *assurance*. Security functionality requirements are those that that must be met in order to provide protection for information (e.g. from the perspective of confidentiality, integrity, or availability) that is stored, processed, or transmitted by an information system or device. Assurance requirements are those that must be met in order to obtain credible assurance that security functional requirements are being met. For example, a computer operating system may implement discretionary access control (DAC) as a security feature for restricting and controlling access to information. Accordingly it may have assurance requirements, such as auditing mechanisms and account review procedures for determining if access control mechanisms are indeed being enforced.

The measures of information security produced by system evaluation methods are qualitative indicators that are assigned based on a set of security functional and assurance requirements that the system fulfills. Figure 2-6 illustrates the general system evaluation process.

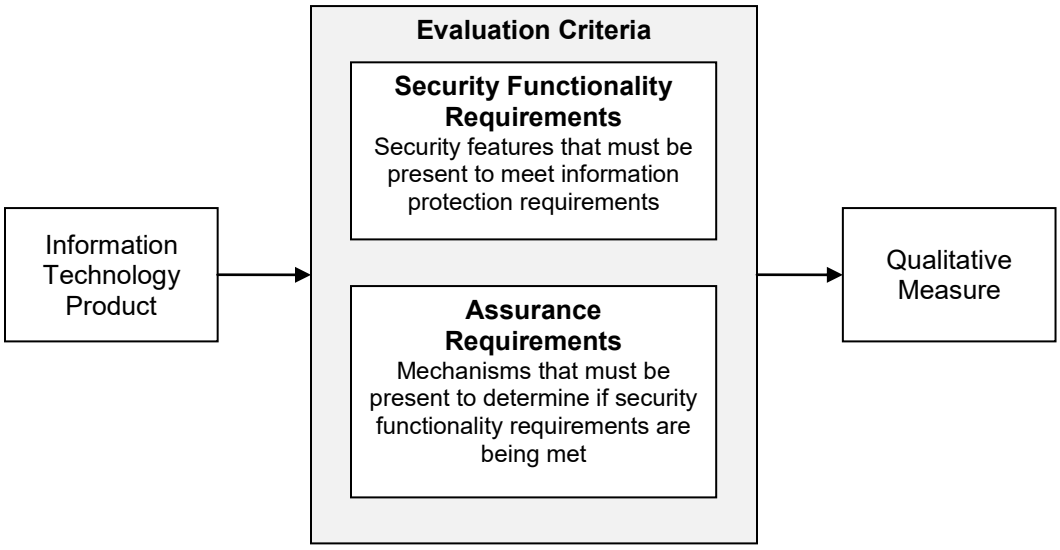


Figure 2-6 General context of system evaluation approach

There are three primary standard evaluation methodologies have either been applied in the past or are currently being used in practice today. They are:

1) The Trusted Computer System Evaluation Criteria (TCSEC)
2) The Information Technology Security Evaluation Criteria (ITSEC)
3) The Common Criteria for Information Technology Security (CC)

2.4.1 Trusted Computer System Evaluation Criteria

The TCSEC was one of the first attempts at a standardized methodology for assigning a *measurement* to the level of security provided by a computer system. Referred to as the "orange book", TCSEC was the overarching document in the Rainbow Series of computer security publications developed by the National Computer Security Center for the Department of Defense (DoD) throughout the 1980's and 1990's. One of the primary objectives of the TCSEC was to provide a metric that would indicate the degree of trust that could be placed in computer systems processing classified or other sensitive information (DoD, 1985). For example, a computer system given the measure of TCSEC C1 indicates that it fulfills the combination of security functional and assurance requirements required for Discretionary Security Protection. The measures provided by the TCSEC are shown in Table 2-3.

Table 2-3 Summary of TCSEC measures of trust, as found in (DoD, 1985)

Level of system assurance & confidence in information protection capability: - (top) to + (bottom)

Division	Name	Class
D	Minimal Protection	Contains evaluated systems that fail to meet requirements for a higher level of assurance
C	Discretionary Protection	C1: Discretionary Security Protection C2: Controlled Access Protection
B	Mandatory Protection	B1: Labeled Security Protection B2: Structured Protection B3: Security Domains
A	Verified Protection	A1: Verified Design

The primary evaluation target for the TCSEC is a *trusted computing base*, defined as the collection of mechanisms *within a computer system* that are responsible for enforcing security policy, such as hardware, software, and firmware (DoD, 1985). As a result, the TCSEC is primarily focused on the technical safeguards within a computer system, such as those built into an operating system. In addition, the TCSEC evaluation requirements are largely focused on access control and the protection of information from unauthorized disclosure. Although this makes them more applicable to confidentiality as opposed to other types of protection, it does not adequately address other types of safeguards, such administrative, personnel, and physical, which exist outside of the trusted computing-base (Chapple, Stewart, and Tittel, 2005). As a result, the relative contribution of these types of safeguards to confidentiality cannot be directly determined. This concept is illustrated in Figure 2-7.

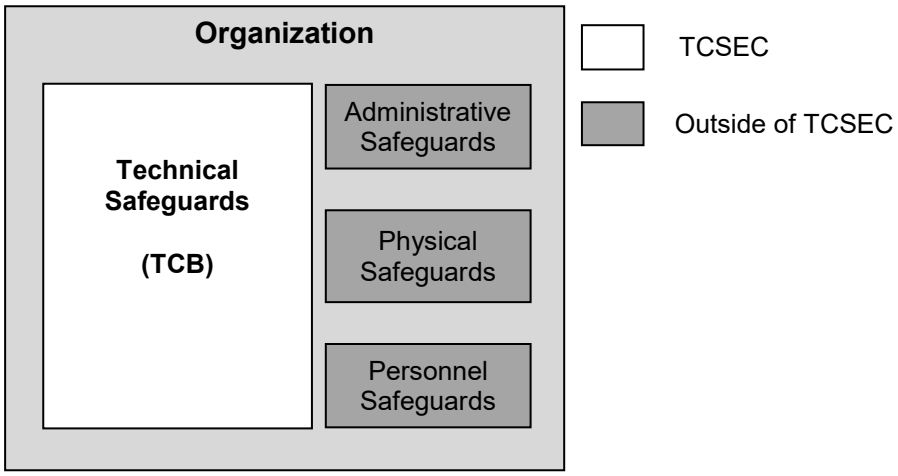


Figure 2-7 Types of safeguards addressed by the TCSEC

2.4.2 Information Technology Security Evaluation Criteria

ITSEC is the result of a European effort to standardize computer security evaluation criteria and measurement methodologies. Published in 1991 as the *Provisional Harmonized Criteria*, the ITSEC was constructed to build on and expand the foundation established by the TCSEC by addressing integrity and availability, in addition to the confidentiality of information resources.

The ITESEC provides separate measures for security functionality and assurance, as opposed to the single consolidated measure provided by the TCSEC. The functional and assurance measures provided by the ITSEC evaluation methodology and the TCSEC equivalents are show in Table 2-4.

Table 2-4 ITSEC functionality and assurance measures and TCSEC equivalent (ITSEC, 1991)

- Level of system assurance & confidence in information protection capability +

ITSEC Functionality Class	ITSEC Assurance Level	TCSEC Equivalent Measure
N/A	E0	D
F-C1	E1	C1
F-C2	E2	C2
F-B1	E3	B1
F-B2	E4	B2
F-B3	E5	B3
F-B3	E6	A1

An advantage of ITSEC over TCSEC is that it is constructed to be more applicable to whole systems operating within commercial environments, unlike TCSEC which was more applicable to proprietary DoD computer systems and technical safeguards (Jahl, 1991). The key indication is that ITSEC does not require that safeguards be isolated within the concept of a trusted computing base (Chapple, Stewart, and Tittel, 2005). However, although the security functional and assurance requirements are designed to address confidentiality, integrity, and availability, indications of the individual types of protection are not discernible from the final measure.

The ITSEC also explicitly makes the distinction between *systems* and *products*, giving consideration to the notion of an observable and operational environment in which targets of evaluation reside. ITSEC explicitly states that systems are designed with specific end-user requirements in mind, and that real-world security threats to them can be determined (ITSEC, 1991). Products are based on more general assumptions, and are designed to fit a number of environments. In this study, we are interested in systems as opposed to specific products. ITSEC does not offer a solution for how system environments, presumably subject to complexity and dynamics, can be accounted for in the evaluation methodology.

2.4.3 Common Criteria for Information Technology Security Evaluation

The Common Criteria for Information Technology Security Evaluation (referred to as the CC), is the latest attempt to standardize security evaluation criteria and methodologies. It is the current international standard, classified as ISO 15408, and effectively replaces the TCSEC and ITSEC. The CC attempts to the address confidentiality, integrity, and availability of a Target of

Evaluation (TOC) through evaluations of security functional and assurance requirements. The CC assigns a single qualitative evaluation assurance level (EAL) based the results of the evaluation. The CC EALs are listed in Table 2-5.

Table 2-5 CC evaluation assurance levels (Common Criteria Part 1: Introduction and General Model, 2009)

	CC EAL	Description
-	EAL0	Inadequate Assurance
Level of system assurance & confidence in information protection capability ↓	EAL1	Functionally tested
	EAL2	Structurally tested
	EAL3	Methodically tested and checked
	EAL4	Methodically designed, tested, and reviewed
	EAL5	Semi-formally designed and tested
	EAL6	Semi-formally verified design and tested
+	EAL7	Formally verified design and tested

The evaluation of a TOC using the CC assumes a 100% correct instantiation of security objectives for the operational environment in which the TOC resides (Common Criteria Part 1: Introduction and General Model, 2009). This highlights a deeper issue with system evaluation methods in general - that they are better suited for the certification and measurement of security for individual information technology *products*. As indicated by Whitmore (2001), the CC

security functional requirements, because of their product-specific nature, are limited in their ability to describe end-to-end security and their use in complex IT solutions is not intuitive.

Andersson, Hallberg, and Hunstad (2004) propose an extension of the CC for the purpose of assessing the *securability* of components in a distributed information system. The authors propose a weighting matrix that assigns CC security functional requirements to confidentiality, integrity, and availability for the purpose of generating quantitative metrics. However, the authors conclude that their method is limited in its current state by the inability to handle the complexity associated with system-wide evaluations in an operational environment.

2.4.4 System Evaluation Methods Summary

While system-evaluation methods are appropriate for the certification and measurement of security with respect to individual information technology products, it is difficult to extrapolate these approaches for complex organizational environments. The underlying approach of functional and assurance requirements is more-applicable for validating product designs against vendors assertions of security-related functionality, as opposed to measuring confidentiality in complex organizational systems consisting of people, processes, and technology.

While system evaluation methods offer a standardized measure of information security, the measures are qualitative and broad, and the various types of protection are not discernible from the final measure. The lack of consideration for the dynamics and interactions among information security-related elements increases the difficulty associated with extrapolating these methods for the measurement of security in a containing or organizational environment.

Additional shortcomings with system-evaluation methods are related to the lack of an underlying information security model that adequately considers *all* types of protection and safeguards, including those related to administrative and physical protection mechanisms.

2.5 Process-Based Approaches

Process-based approaches have also been applied to generate measurements of information security. The most notable is the Systems Security Engineering Capability Maturity Model (SSE-CMM), which is a community-owned process reference model for assessing the *maturity* of systems security engineering processes (SSE-CMM, 2003). The general hypothesis of process-based approaches is that the more mature an organization's security-related processes are, the more likely they are to exhibit desirable characteristics.

The SSE-CMM identifies *Process Areas* for system security engineering, such as "Administer Security Controls" and "Assess Threats". Each process area consists of Base Practices, which are defined as essential characteristics (i.e. activities) that must exist within security engineering processes. Similar to the systems engineering and software engineering capability maturing models, the SSE-CMM defines five maturity levels for security engineering processes. The SSE-CMM maturity levels are identified in Table 2-6.

Table 2-6 SSE-CMM maturity levels

Maturity	Description
Capability Level 1	Performed informally
Capability Level 2	Planned and tracked
Capability Level 3	Well defined
Capability Level 4	Quantitatively controlled
Capability Level 5	Continuously improving

Keblawi and Sullivan (2007) argue that determining security processes, both effective and ineffective, may represent a more practical approach for analyzing information security within an organization than assessments of information security safeguards. Indeed, processes are an important element of organizational information security. However, processes alone cannot maintain confidentiality, as their implementation implies interactions with people and technology.

Huang and Nair (2008) propose a mapping of the safeguard standards identified in the HIPAA Security Rule to the base practices identified in the SSE-CMM for the purpose of developing a risk assessment process for patient-centered healthcare systems. Although not specific to healthcare, Liang and Ming-Tian (2006) use a similar technique for developing a security evaluation approach based on a mapping between Common Criteria functional and assurance requirements and the process areas of the SSE-CMM. While novel, these approaches are subject to the same challenges identified with the compliance-based and system evaluation methods discussed in Sections 2.3 and 2.4, respectively.

2.5.1 Process-Based Summary

Process-based methods are advantageous in that they address activities that support information security. However, the capability of a process alone does not provide an adequate indicator of information security within an organization. The types of measures and metrics offered by approaches such as the SSE-CMM are qualitative and broad, and are limited in their ability to measure information security in terms of the requisite protection perspectives identified in information security standards, such as confidentiality.

2.6 Dependability Techniques

Dependability concepts and evaluation techniques have been extended for the purpose of generating measures of systems security. These techniques are similar to those used for obtaining measures of other system-level properties, such as reliability and safety. Before moving into the specific types of concepts and techniques being extended, a brief overview of dependability is provided.

2.6.1 Dependability Concepts

The first formal taxonomy for dependability was published in 1992 in an effort to synthesize previous research efforts and define standard concepts and terminology for what constitutes fault-tolerant and dependable computing. Dependability is defined as the trustworthiness of a computer system such that reliance can justifiably be placed on the service that it delivers (Laprie, 1992). A service is the system's behavior as it is perceived by other

systems (human or physical) with which it interacts. The systems behavior is determined by its structure.

The concept of dependability has evolved from the foundations documented in Laprie (1985) to include more rigorous definitions, descriptions, and consideration of security-related concerns. The continued convergence of dependability and security was captured by Avizienis, Laprie, Randell, and Landwehr (2004) in their updated taxonomy of dependability and security. The security and dependability tree is shown in Figure 2-8.

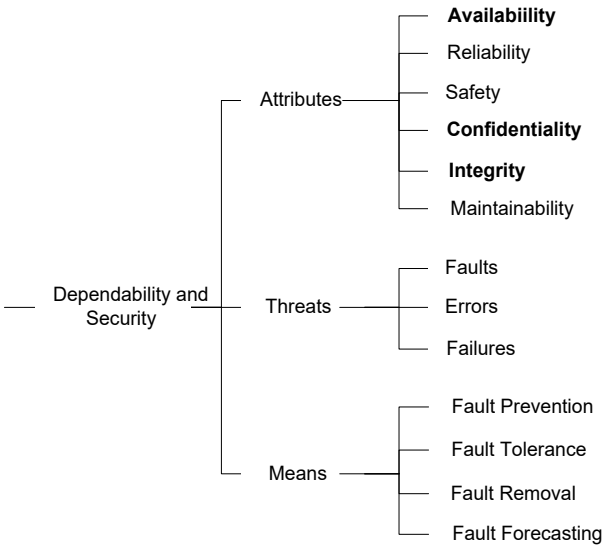


Figure 2-8 Dependability and security tree (Avizienis et al, 2004)

As shown in Figure 2-8, dependability consists of three primary components: attributes, impairments, and means. Attributes enable the expression of system properties and permit the assessment of system quality resulting from threats and the means that oppose them. The

dependability of a system is characterized in terms of its attributes. The security-specific attributes of dependability are confidentiality, integrity, and availability. The definitions for these attributes are consistent with the standard definitions for confidentiality, integrity, and availability provided in Chapter 1.

Threats are undesired circumstances under which reliance can no longer be placed on the service delivered by a system. An example of a typical information security threat was discussed in Section 2.1.1. Three primary types of dependability impairments are faults, errors, and failures.

Means are methods that provide the ability to deliver services on which reliance can be placed. In addition, means assist in achieving confidence in the ability of system to deliver these services. Means can be thought of as safeguards.

Dependability concepts for information security measurement and evaluation are advantageous because they are based on more-rigorous system concepts than the other approaches for addressing information security measurement discussed earlier in this chapter. Recall that one of the primary shortcomings is that these approaches lack adequate consideration for an operational environment and the dynamic nature of systems. As noted by Laprie (1992), dependability concepts are not to be restricted to systems with static and unchanging structures, but should allow for structural changes that result from threats. This gives rise to the notion of system states. With respect to information security, we see this in the form of the threats and vulnerabilities which predicate new protection requirements and safeguards for mitigating the potential adverse impacts to information resources.

The two primary dependability evaluation techniques have been extended for the purpose of generating measures of systems security are combinatorial methods and state-space methods.

2.6.2 Combinatorial Methods

2.6.2.1 Attack Trees

Attack trees (also referred to as attack graphs) are security-related extensions of fault trees, which have traditionally been used to perform reliability and safety analysis. Like fault trees, attack trees identify the possible events or conditions that contribute to a system failure. In the case of information security, a system failure is synonymous with a compromise or breach of information resources. Attack trees can be represented textually, but are more commonly represented in graphical form.

The root node in an attack tree represents the ultimate goal of an attacker, and child nodes (non-leaf nodes) represent the sub-goals that an attacker must achieve for the attack to be successful. Each non-leaf node is characterized as either "AND" which indicates that a set of sub-goals must be achieved for a successful attack, or "OR" which indicates multiple ways that a successful attack can be achieved. Figure 2-9 illustrates the generic structure of "AND" and "OR" nodes (Moore et al, 2001), and provides a trivial example of an attack tree, in which unauthorized database access is the ultimate goal of the attacker.

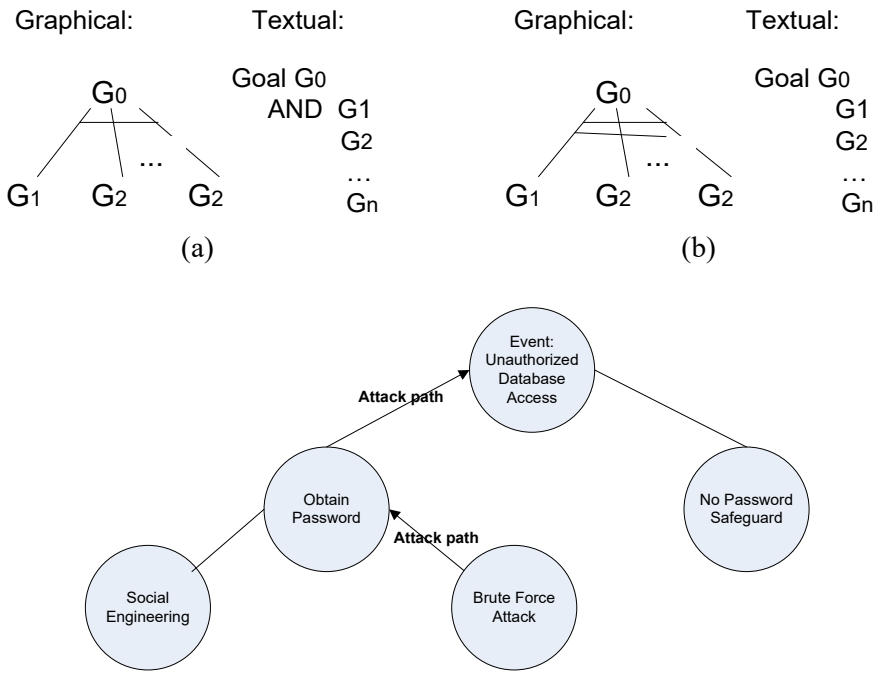


Figure 2-9 Attack trees (a) AND (b) OR nodes (Moore et al, 2001); (c) simple example

Attack trees are advantages in they can be used to model *attack paths* for a given system or collection of systems. Based on the values assigned to the nodes (e.g. time to complete goal, cost to complete goal, probability of goal completion), measures of information security can be generated. For example, nodes could represent system vulnerabilities specific to confidentiality, integrity, or availability. Measures of information security can be calculated by evaluating the corresponding attack paths.

2.6.3 State-Space Methods

2.6.3.1 Model Checking

Nicol et al (2004) and Atzeni and Lioy (2005) identify the use of model-checking techniques as an approach for developing measures of systems security. Model checking techniques are concerned with the *reachability* of possible states that are implied by some formal expression of a system. The general approach involves applying algorithms that explore the entire state space and provide knowledge regarding the sequence of transitions required to reach a state of interest. Ammann and Ritchey (2000) present an application of model checking in which a network security model is constructed using information regarding the interconnectivity and vulnerabilities of network hosts, in addition to attacker access levels. Model checking tools are used to explore the state space and identify the specific sequences of transitions that disprove assertions of security (e.g. the specific sequences of vulnerabilities that must be exploited are identified).

Model checking is advantageous in that it offers an approach for generating measures of information security by validating, or conversely disproving security-related assertions. For example, the number of actions (transitions) required to compromise an information resource can be used to measure security as a function of attacker effort. However, model checking techniques are similar to other state-based approaches in that the analytical feasibility is impacted by the size of the state-space. As a result, caution must be exercised in attempts to scale these efforts to large and complex systems.

2.6.3.2 State-Based Stochastic Methods

State-based stochastic methods are advantageous in that they use *stochastic* modeling techniques, such as Markov Chains, for addressing the non-deterministic nature of systems. The ability to capture aspects of system behavior can help to overcome the limitations of existing formal methodologies for information security measurement.

Helvik, Knapskog, and Sallhammar (2006) use stochastic game theory to compute a measure of expected attacker behavior based the concept of rewards and cost. System intrusions (the result of intentional and malicious faults) are modeled as transitions between system states in a stochastic game. The approach is based an assumption that the attacker has complete knowledge of all system states, including transitions between states and existing vulnerabilities, which by the authors admission, is not always the case in real-world applications.

Dacier, Deswarte, and Kaâniche (1996) transform a *privilege graph* into a stochastic Petri Net from which a Markov chain describing the potential intrusion states is derived. Security measures are then derived using a reachability graph. It is the belief of the authors that the effort and time spent by an attacker are sufficient measures for characterizing security in terms of the intrusion process.

Trivedi et al (2009) further extend dependability concepts by presenting an extended classification of threats and mitigation techniques. The authors develop composite model types for dependability attributes based on the extended classifications. It is shown that these model types can be constructed and evaluated using the approaches that were identified in Sections 2.6.2 and 2.6.3. For example, a confidentiality-reliability state model is presented by the authors.

State-based methods can be used to model complex relationships, while capturing state transition structure and sequencing information (Nicol et al, 2004). However, a disadvantage of state-based approaches is that complex systems consisting of many components and interactions can create a large number of potential states. Each state represents a condition that may need to be addressed through a new security requirement or safeguard, which increases the difficulty associated with information security measurement (Cunningham and Pfleeger, 2010). A large number of states, which is predicated not only by systemic complexity but also by the changing nature of threats to electronic information, represent significant challenges in analyzing models of "real-world" systems. As a result, exhaustive state models for information security measurement approaches *may be infeasible*, and *good* solutions should be employed to overcome the associated challenges.

2.6.4 Dependability Summary

Dependability techniques offer a promising approach for security measurement as they are derived from existing quantitative approaches for calculating system-level properties such as reliability. In addition, they introduce more-formal system definitions and concepts into the problem domain of information security measurement. However, as previously discussed, these methods are currently limited by their scalability to complex systems, particularly in the case of exhaustive state-space searches.

2.7 Summary of Existing Methodologies

Table 2-7 provides a summary of the information security measurement approaches analyzed in this chapter. Each approach is described in terms of the type of measure (qualitative/quantitative) that it produces, whether it supports a separate measure for confidentiality, and if the measures are derived from an underlying system model.

Table 2-7 Summary of methodologies and approaches for information security measurement

Approach	Quantitative/ Qualitative	Exclusive Measurement For Confidentiality	Measure Derived from System Model
Compliance-Based[1]	Mixed	No	No
TCSEC[2]	Qualitative	No	No
ITSEC[2]	Qualitative	No	No
CC[2]	Qualitative	No	No
SSE-CMM[2]	Qualitative	No	No
Dependability[3]	Quantitative	No	No

Type:1-common 2-standard 3-experimental

2.8 Conclusions

In this chapter, healthcare information security standards and the general types of methodologies for information security measurement were reviewed. Based on this analysis, it appears that a standard approach for measuring the confidentiality of electronic information in healthcare-related organizations has not been established. Although several classes of approaches and methodologies are available for measuring information security in general, there are

underlying deficiencies that preclude their direct adaptation to the problem stated in Chapter 1. These deficiencies are not unique to healthcare organizations, but are representative of the challenges facing any organization that seeks to measure confidentiality in an enterprise context. The key issues affecting information security measurement methodologies that were synthesized from the literature review are identified in Table 2-8.

Table 2-8 Summary of key issues affecting information security measurement methodologies

Issue	Underlying Cause	Synthesized From
Current approaches do not delineate how well an organization is performing in a particular protection perspective, such as confidentiality.	There is a lack of approaches for measuring information security perspectives in the context of an information security model. Current methodologies typically treat information security as a generalized concept and information security standards do not provide an approach for measuring the different desired protection perspectives that are identified.	-General impression -HIPAA Security Rule for EPHI -NIST SP 800-66 -Wang, 2005
Current approaches do not account for the contributions made to a protection perspective by safeguards and the organizational components of people, processes, and technology.	Current methodologies offer little insight into how safeguards, people, processes, and technology contribute to a system of protection. There is a lack of foundational models on which measurements of information security can be based. The lack of a standard or foundational reference models inhibits consistency across approaches for information security measurement.	-General impression -Wang, 2005 -Vaughn et al, 2001 -Hessami and Karcanias, 2009
Current approaches do not account for the complex and dynamic nature of information security contributors and safeguards.	Information security is a complex and dynamic concept, in which multiple people, process, and technology contributors interact with safeguards in order to protect electronic information. Measurement approaches do not account for these types of interactions and as a result measurements of information security are not truly reflective an organization's ability to maintain the confidentiality of electronic information.	-General impression -Cunningham and Pfleeger, 2010 -Wang, 2005 -DHS, 2009 -Nicol, et al, 2004 -Verendel, 2009

CHAPTER 3

METHODOLOGY

3.1 Introduction

In Chapter 1 and Chapter 2, the problem space surrounding the protection of electronic information was explored and the key issues as they relate to the measurement of confidentiality were presented. In this chapter, a solution is formulated which attempts to address some of these issues. The approach consists of synthesizing an information security system (ISS) from the HIPAA Security Rule safeguards and the people, processes, and technologies which contribute to their realization from the organizational space. A desired emergent property of the ISS – confidentiality - is characterized in terms of the systemic interactions which are present. By quantifying these interactions, a confidentiality measure is defined which indicates the level of protection from the unauthorized disclosure of electronic information. This chapter is intended to establish the solution approach and underlying theory. A system model for demonstrating the proposed solution is developed and demonstrated in Chapter 4 and Chapter 5, respectively.

The remainder of this chapter is constructed as follows: Section 3.2 provides an overview of the solution framework utilized in this chapter. Section 3.3 provides a background on systemic thinking and information security in order to supply the relevant theory surrounding the proposed approach for measuring confidentiality. In Section 3.4, an ISS is synthesized by investigating systemic characteristics that are present within the organizational problem space. Section 3.5 defines an ISS in terms of its properties, and provides the corresponding approach for calculating

confidentiality. Section 3.6 presents a confidentiality metric based on the measurement approach, and Section 3.7 concludes the chapter by providing a summary of the work completed.

3.2 Overview of Solution Framework

The solution for measuring the confidentiality of electronic information in healthcare-related organizations developed in this research is designed to address healthcare information security standards and to address, in part, the underlying issues with existing information security measurement approaches. Because the HIPAA Security Rule is the primary healthcare information security standard, it is critical that healthcare-related organizations are able to address confidentiality from the perspective of this benchmark. In addition, it is also necessary to develop a solution which attempts to address the shortcomings with existing approaches for general information security measurement.

3.2.1 Requirements for Solution Approach

Using the top-level research objective stated in Chapter 1 and the underlying issues with existing measurement approaches identified in Table 2-8, four overarching requirements for a solution approach were derived. These requirements frame the solution approach developed in this chapter and are identified in the following subsections.

3.2.1.1 Healthcare-Specific Needs

The solution should address the information security standards and safeguards identified in the HIPAA Security Rule for EPHI. Healthcare-related organizations are in need of better approaches for measuring information security, specifically confidentiality, as they experience continued growth in healthcare information technology and migration toward electronic health records. There are increasing demands for organizations that utilize digital patient information to demonstrate both compliance with industry standards and to address stakeholder concerns regarding the confidentiality of personal medical information.

3.2.1.2 Systemic Thinking

The solution should utilize systemic thinking and concepts to address the dynamic and complex nature of information security. Such approaches are beneficial for investigating and capturing elements and related concepts in an otherwise disjoint problem space. Systemic tools and methods are also beneficial for understanding the nature of emergent properties as features of aggregation in complex systems, and the degree of their presence or absence (Hessami and Karcanias, 2009). As a result, systemic thinking is a key concept for understanding how confidentiality emerges from information security-related elements that are present within the organizational problem space.

3.2.1.3 Protection System Concept

The solution shall consider information security as a system that resides within a larger organizational system. Current methodologies and approaches for information security

measurement do not clearly delineate the system *providing the security* from the *system being secured*. Humans, technology, and processes should be considered as part of any measurement approach for confidentiality as they contribute to protection mechanisms designed to prevent the unauthorized disclosure of electronic information. In general, security should be viewed in the context, purpose, and value of the larger system being secured (Fox, Henning, and Vaughn, 2001). In addition, establishing a system of protection facilitates the ability to evaluate this system in terms of its properties.

3.2.1.4 Delineation of Measurement

The solution shall provide a separate measure for confidentiality. Current measurement methodologies may address confidentiality, but it's typically indistinguishable from other security properties because information security is viewed as a generalized concept.

3.2.2 Solution Framework

Each top-level requirement was mapped into a solution framework, consisting of three primary steps. Each step corresponds to a component of the solution developed in this chapter.

3.2.2.1 ISS Synthesis

In this step, systemic thinking and concepts are applied to synthesize complex, dynamic, and emergent characteristics among people, processes, technology and safeguards. The objective of this step is to delineate the protection system that resides within the containing organization by capturing systemic elements and interactions that are present.

3.2.2.2 ISS Confidentiality Measure

The objective of this step is to formalize the structural definition of an ISS, and quantify the interactions that occur among the safeguard and contributor elements that are present. This constitutes the approach for calculating confidentiality as an emergent property of the ISS.

3.2.2.3 Confidentiality Metric

The objective of this step is to define a metric for confidentiality based on the measurement approach. Figure 3-1 provides an illustration of the solution requirement-to-framework mapping.

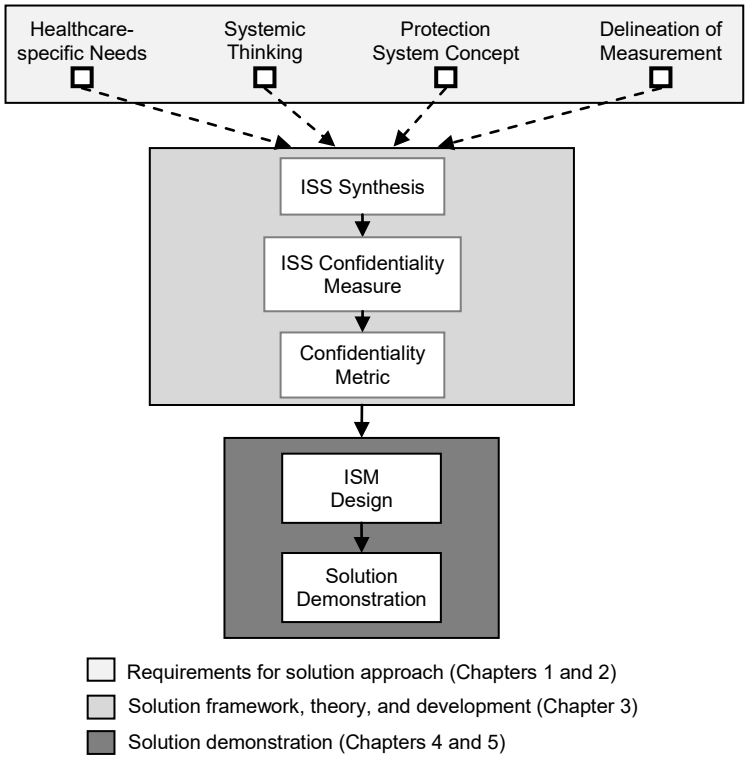


Figure 3-1 Mapping of solution requirements to solution framework

3.3 Systemic Thinking and Information Security

The solution developed in this chapter adopts a *systemic* perspective on the subject of information protection, in which information security is viewed as a *system* with desired *emergent* properties. In the context of information security, a "system" is traditionally viewed as a physical and tangible protection mechanism, such as a network infrastructure device or suite of access control software. This approach is more-consistent with a "hard" view of *systems thinking* which, according to Checkland (2000), assumes that the world is a set of systems (i.e. is systemic) and that these can be *systematically engineered* to achieve objectives. For example, a firewall can be designed based on a set of customer requirements. The combination of hardware and software that it is composed of can be developed, tested, and configured until it fulfills specific functional objectives related to the control of network traffic. In addition, business processing applications, such as EHR software, are representative of these types of systems.

However, organizational information security is a much broader and complex issue. When attempting to measure information security in an organizational context, one must look beyond the individual security mechanisms contained within a set of hard, physical systems and focus on the environment which surrounds these systems. As discussed in Section 2.1.1, this is referred to as the general control environment and it establishes the organization's enterprise-wide approach for protecting the electronic information that it maintains. This environment can be thought of as a conceptual protection space which exists throughout the overarching organizational environment.

A key principle of the approach developed in this chapter is that a solution for measuring confidentiality subsists within this complex environment and can be synthesized from the

elements and related concepts which are present. Figure 3-2 illustrates the key elements of the general control environment that are present within the containing organizational environment.

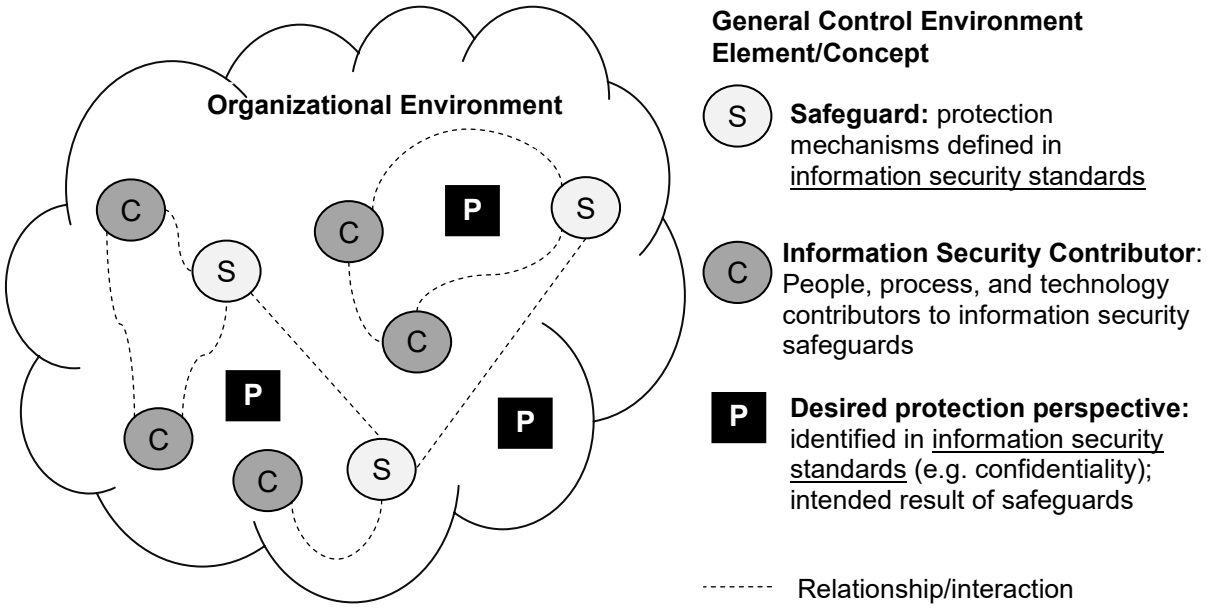


Figure 3-2 Information security elements and concepts within the organizational environment

As shown in Figure 3-2, information security safeguards and the people, process, and technology contributors to these safeguard are present within the organizational environment. Additionally, desired protection perspectives are indicated as they are the *intended* result of implementing a set of safeguards. Although safeguards and contributors are distributed throughout the organizational space they are interrelated, and an organization's ability to maintain desired protection perspectives is dependent upon their ability to function as a *whole*. This whole is defined as an ISS, and the desired protection perspectives are viewed as desired

emergent properties of this system. Specifically, confidentiality emerges due to the structure and interactions of hierarchical elements (i.e. systems and subsystems) that define an ISS and delineate it from the overarching organizational environment. As a result, the measure of confidentiality produced by this solution indicates the degree to which confidentiality exists within the ISS. This indicator is appropriate as it provides insight regarding the *function* of a *protection system* as opposed to that of an individual hardware or software element, and allows for a more rigorous understanding of the relationship between the required safeguards and desired protection perspectives identified in information security standards. In addition, this approach extends beyond typical studies of organizational information security controls (i.e. safeguards) which, according to Baker and Wallace (2010), have focused on their presence or absence, as opposed to deeper investigations of the quality of these mechanisms.

3.4 ISS Synthesis

In this section, the organizational environment depicted in Figure 3-2 is investigated to identify the systemic elements and interactions that are present and how they lead to the emergence of desired characteristics. This is essential for delineating an ISS from the containing organization, and defining the relevant structural and behavioral attributes necessary for property measurement.

As described by Hitchins (2007), the *synthesis* of systems with desired emergent properties yield an evident relationship between the systemic precepts of *complexity*, *dynamics*, and *emergence.* First, we investigate the types of complex and dynamic characteristics that are

manifest among information security contributors and safeguards, and then discuss how this leads to the emergence of desired protection perspectives.

3.4.1 Complexity

3.4.1.1 Contributor-Safeguard Complexity

Although safeguards may vary across information security standards, the elements that contribute to their realization are not unique, but are fundamental to all organizations. A safeguard requires the contributions from one or more information security *contributors*, which are defined as people, process, or technology elements. The diagram shown in Figure 3-3 illustrates an example of the typical people, process, and technology contributors to the HIPAA Administrative safeguard "Access Authorization"

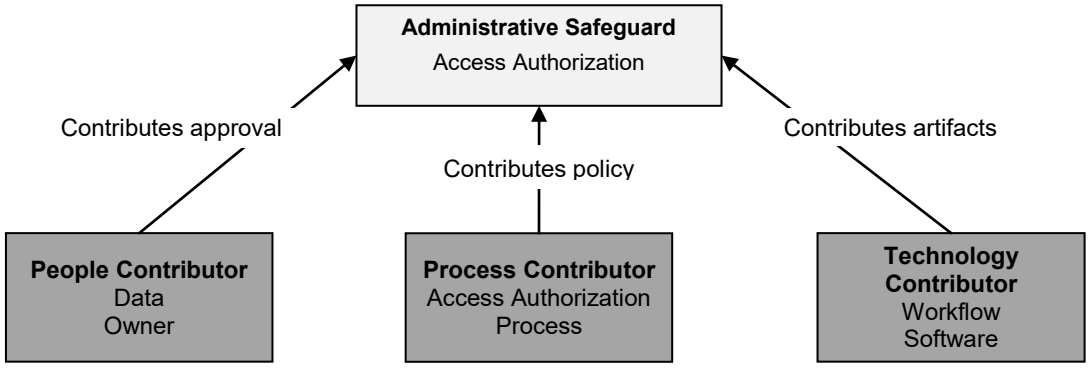


Figure 3-3 Example of information security contributor complexity

The access authorization safeguard is a standard protection mechanism implemented by organizations for authorizing (i.e. approving) a users access to electronic information. The overarching objective is to mitigate the risk of unauthorized access, making it a confidentiality-based safeguard. It involves 1) determining if access is necessitated by job responsibilities and 2) granting the required approvals in a manner defined by organizational information security policy.

As shown in Figure 3-3, the access authorization safeguard requires contributions from people elements (e.g. data owner for providing approval of access requests), processes elements (the steps that comprise the access authorization policy), and technology (workflow software for maintaining artifacts of the authorization process). A failed or reduced contribution from any contributor reduces the safeguard's efficacy in maintaining confidentiality. For example, the ability to approve access requests should be restricted to authorized individuals. Otherwise, the lack of control over *who* approves access results in a lack of control over *who access is granted to.* The resulting condition is an ineffective safeguard, and subsequently a loss of confidentiality as there is now a reduced level of assurance that access is restricted to authorized individuals. Also, if proper artifacts are not maintained, access requests and the corresponding approvals cannot be substantiated, which significantly impacts the ability to perform meaningful information security audits or after-the-fact investigations necessitated by security incidents regarding confidentiality.

3.4.1.2 Safeguard-Safeguard Complexity

In addition to the complexity among information security contributors, there is also complexity that is present among the safeguards required by information security standards. For example, the HIPAA safeguard Access Authorization is related to other confidentiality-based safeguards identified in the HIPAA Security Rule such as "Termination Procedures" (administrative-type safeguard) and "Unique User Identification" (technical-type safeguard). Figure 3-4 provides an example of the complexity that exists among the HIPAA information security safeguards.

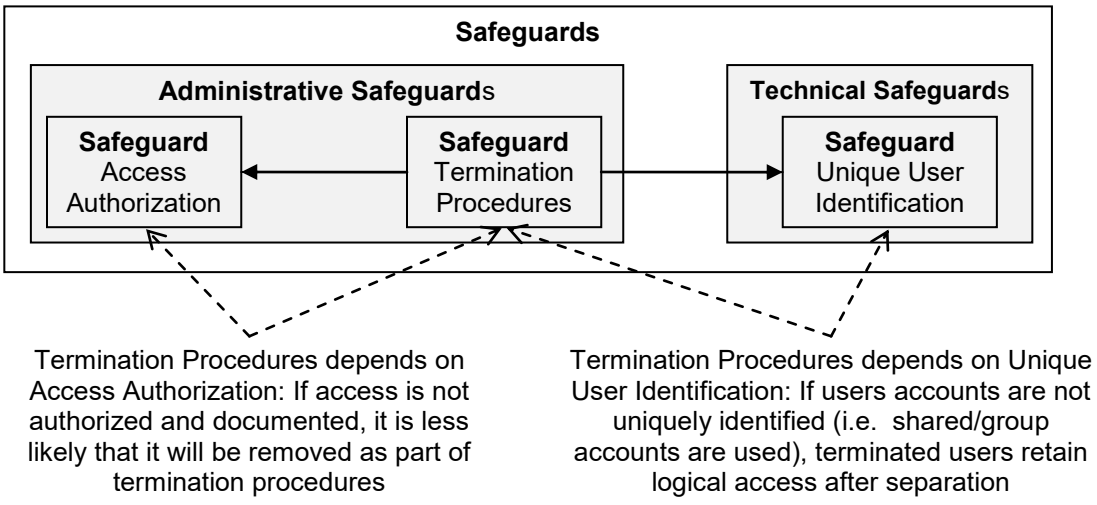


Figure 3-4 Example of complexity among HIPAA administrative and technical safeguards

The illustration shown in Figure 3-4 indicates the types of interactions or *dependencies* that exist among safeguards and safeguard types. These interactions are critical to the protection of electronic information. For example, Termination Procedures consist of the steps (i.e. the

policy) to be followed when an employee leaves an organization. This safeguard supports confidentiality, as one of its primary purposes is to remove the logical access of individuals at which point they are no longer *authorized* to view electronic information that is maintained by an organization.

However, an inadequate access authorization safeguard reduces the likelihood that a user's access is formally documented, such as when access to specific applications or network resources is granted without being approved. In this case, it is less likely that security personnel will know to remove the access upon employee separation, as they would have to review every application to determine which accesses were held. Inappropriate network access and delayed termination of employee network access are two common examples of general control deficiencies that have been identified in DHHS Office of Inspector General (OIG) audits of existing healthcare organizations for which DHHS has oversight (DHHS, 2011).

Safeguards that address termination procedures are also dependent on the technical safeguard "Unique User Identification", which addresses the assignment of unique authenticators (e.g. usernames and passwords, or access tokens) to information systems users. If adequate policy and corresponding processes for identity management do not exist, there is a lack of control over the use of group or shared information system accounts. Group and shared accounts consist of a single username and password that is shared by multiple individuals. In this case, it is difficult to remove logical access as part of the termination process as the user may retain access even after separation, assuming that the group credentials are not modified following employee separation. Intuitively, this condition is exacerbated when group or shared accounts are not formally justified, documented, and approved per an access authorization process.

3.4.2 Dynamics

3.4.2.1 Contributor-Contributor Interactions

The dynamics that exist among information security contributors *limit* or *constrain* their ability to contribute to safeguards, which affects the degree to which safeguards maintain confidentiality within an organization. For example, if those responsible for approving access (such as a data owner) do not follow the established authorization process, then the corresponding process contribution is constrained by the data owner.

Another example of a reduced safeguard contribution exists in instances in which a data owner creates their own ad-hoc approach for authorizing access, which introduces disparity within the organizational approach to access authorization. Unique processes created in this manner may not be thoroughly examined before adoption and may not correctly enforce overarching information security policy. Figure 3-5 illustrates an example of an interaction between information security contributors in which a process contribution is constrained by a data owner.

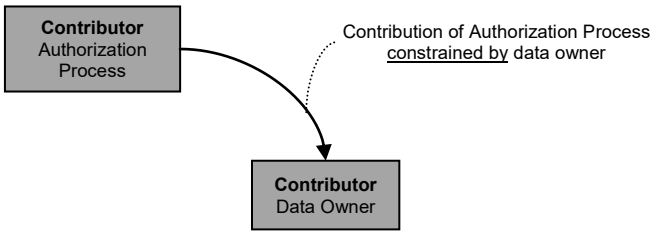


Figure 3-5 Example of information security contributor dynamics

3.4.2.2 Safeguard-Safeguard Interactions

The dynamics, or interactions, that are present among safeguards are critical for maintaining confidentiality within a general control environment. As discussed in Section 3.4.1.2, the efficacy of a safeguard may be impacted by the efficacy of a safeguard on which it depends. For example, if the access authorization safeguard is not receiving the proper contributions from people, process, or technology contributors, the efficacy of the termination procedures safeguard is reduced due to dependence that is present among these two safeguards. The illustration shown in Figure 3-6 provides an example of the interactions among safeguards.

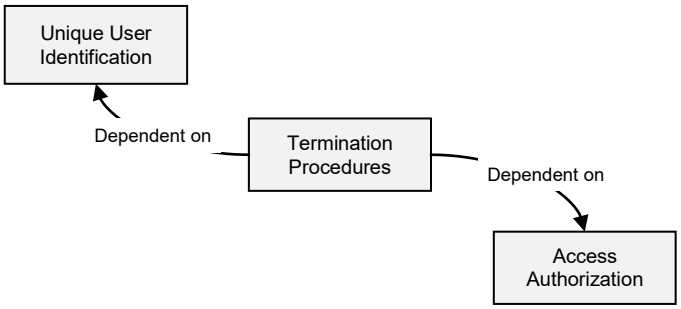


Figure 3-6 Example of safeguard dynamics

3.4.2.3 Contributor-Safeguard Interactions

The interaction among contributors and safeguards were detailed as part of the complexity discussion provided in Section 3.4.1.1.

3.4.3 Emergence

Emergence is a systems-theoretic concept in which a property exhibited by a system is not necessarily discernible from any individual system or component of which it is composed. The existence of emergent properties is predicated on the interactions of contained elements (systems and subsystems) which are conceptually nested within their parent (i.e. containing) system. This structure is referred to as *hierarchy*. Figure 3-7 places the interactions among information security contributors and safeguards identified in Sections 3.4.1 and 3.4.2 in the context of a conceptual protection system which resides within a containing organization.

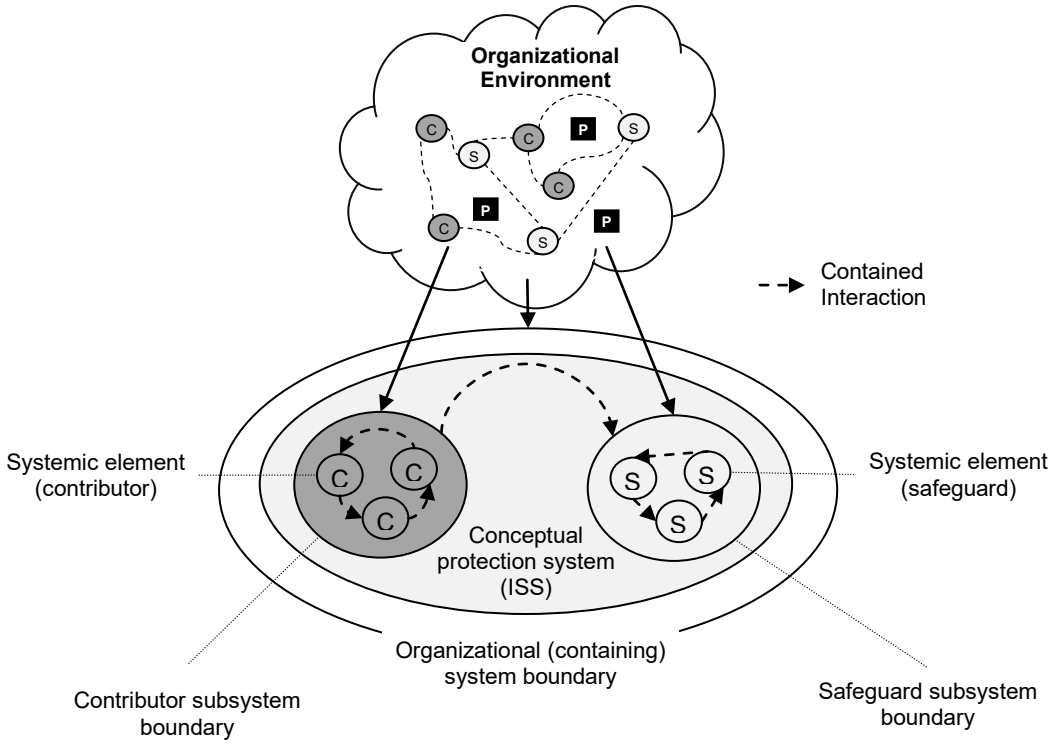


Figure 3-7 Conceptual protection system structure and contained interactions

The existence of a hierarchical structure is evident in Figure 3-7, in which interactions are present at the contributor, safeguard, and protection system levels, all within the containing organization. Because emergence is predicated on the structure and interactions of hierarchical elements, the ISS-level *properties* can be characterized as *emergent* and resulting from the contained interactions within the safeguard and contributor subsystem, and within the ISS-level boundary. These emergent properties are desired and correspond to the protection perspectives identified in the HIPAA Security Rule. Therefore, the set of information-security related properties that characterize the ISS is defined as $\boldsymbol{P} = \{p_1, p_2, p_3\}$ where:

p_1 = confidentiality

p_2 = integrity

p_3 = availability

Although this study is confidentiality-focused, integrity and availability are identified for completeness. This point is made to show that a similar synthesis process can be applied for addressing properties other than confidentiality.

3.4.4 Synthesis Summary

In this section the types of complex, dynamic and emergent characteristics among people, processes, technology and safeguards were investigated. Using these concepts, an ISS was synthesized and delineated from the containing organizational space as illustrated in Figure 3-7. Table 3-1 and Table 3-2 list the types of generalized systemic elements and interactions identified during the synthesis process, respectively.

Table 3-1 Systemic elements table

Systemic Element	Type	Description
Information Security Contributor	People, process, & technology	Element which contributes to the realization of safeguards in the general control environment.
Information Security Safeguard	HIPAA Sec. Rule - administrative, physical, & technical	Element which protects electronic information from confidentiality-based threats to the general control environment.

Table 3-2 Systemic interactions table

Interaction	Type	Hierarchy Level	Description
Contributor-safeguard	Contribution	ISS	Required for realization of safeguards within the general control environment.
Contributor-contributor	Constraint	Contributor subsystem	Occurs among the set of contributors that contribute to a specific safeguard and limits the contributions they provide.
Safeguard-safeguard	Dependency	Safeguard subsystem	Required for confidentiality to be maintained throughout the general control environment.

In the next section, the approach for measuring confidentiality as an emergent property of an ISS using the types of information shown in Table 3-1 and Table 3-2 is presented.

3.5 ISS Confidentiality Measure

The approach for developing a confidentiality measure consists of formalizing the structure of an ISS and quantifying the associated interactions. This is accomplished using the results of the synthesis process discussed Section 3.4. The result is a series of relationships and rules that determine the level of confidentiality within the ISS. Throughout the remainder of this chapter confidentiality is referred to as p_1, as it is discussed in the context of a formal ISS system-level property.

3.5.1 ISS Formalization

Formalizing the ISS consists of mathematically stating the structural relation of safeguards and contributors. These formalizations will facilitate the definition of quantified interactions among these elements which are used for calculating p_1.

3.5.1.1 Safeguards

Within the ISS, there exists a safeguard subsystem which contains n safeguard elements. Let **S** be the set of safeguards in the safeguard subsystem: $\mathbf{S} = \{S_i, S_{i+1 \ldots} S_n\}$ for $i = 1 \ldots n$. Any $S_i \in \boldsymbol{S}$ may be dependent on k other safeguard elements in **S** as described in Section 3.4.2.2. For each $S_i \in \boldsymbol{S}$, let $\mathbf{S_iD} = \{S_d\}$ be the set of safeguards on which S_i depends, where d is the i^{th} index of the corresponding safeguard element in **S**.

3.5.1.2 Contributors

Within the ISS, there exists a contributor subsystem. Each $S_i \in \boldsymbol{S}$ has a set of required contributions that are provided by a set of *m* contributor elements existing in the contributor subsystem. For each S_i, the set of required contributor elements is defined as $\mathbf{C_i} = \{C_{ij}, j=1...m\}$ where C_{ij} is the jth contributor for safeguard *i*. Within $\mathbf{C_i}$, *q* constraint interactions as defined in Section 3.4.2.1 may be present. For each *q*, let $\mathbf{C_iI_q}$ contain the C_{ij} contributor elements that participate in the *q* constraint interactions, where the first element is the element that is "constrained" and the remaining elements are the "constrained by" elements. Figure 3-8 illustrates an example of the safeguard and contributor formalizations.

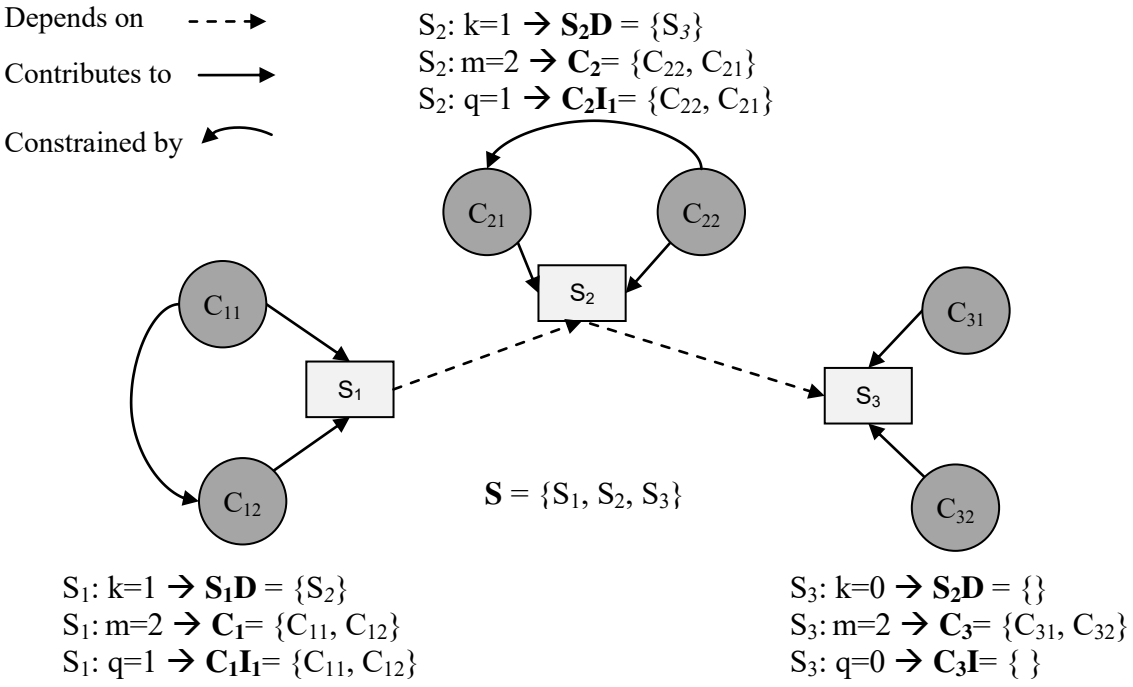


Figure 3-8 Formalized safeguards and contributors (3 safeguard example)

3.5.2 Interaction Quantification

Calculating a measure of p_1 consists of quantifying the safeguard, contributor, and ISS-level interactions identified in Table 3-2. The result is a series of relationships and rules that determine the level of p_1 within the ISS. This section assumes the notation presented in Section 3.5.1. The following assumptions are also established:

- Each $S_i \in \boldsymbol{S}$ is assigned a confidentiality weight (w_{c_i}), a continuous value in the interval [0, 1], which corresponds to the degree in which it addresses confidentiality. The intent of applying a weight is to permit a given safeguard to have more influence in the overall measure of confidentiality than other safeguards. For example, the access authorization safeguard would have a higher weight than safeguards which specifically address integrity-related controls. As a result, the measure of confidentiality should capture this perceived importance.
- Each $C_{ij} \in \boldsymbol{C_i}$ is of equal importance to its respective S_i. Specifically, *no* weight value is assigned to the individual contribution values for a given safeguard. This is consistent with the underlying theory presented earlier in this chapter, in which the importance of each type of contributor for a given safeguard was described.
- The interactions among contributors are considered on a safeguard-by-safeguard basis. Specifically, there is no attempt in this study to formulate an organizational-level model of all contributors. As a result, the interactions defined in each $\mathbf{C_iI_q}$ for a safeguard are independent of those defined for other safeguards.

- The measurement approach does not attempt to build-in models of human behavior when considering the interaction among contributor elements. The measurement approach recognizes the importance of people, process, and technology interactions and attempts to address the effect on safeguard contribution values predicated by these interactions. It is envisioned that these types of models could be integrated into the approach developed in this study as part of future research efforts.

3.5.2.1 Contribution-Type Interaction

Each $S_i \in \boldsymbol{S}$ has a *contribution score* which captures the contributor-to-safeguard (contribution-type, ISS-level interaction) interaction. The contribution score is number of *contribution units* present relative to the total required for a safeguard. Each safeguard has *m* required contribution units, 1 for each required contributor. Each contributor provides a C_{ij-CTR} value, where C_{ij-CTR} is the contribution value ($0 \leq C_{ij} \leq 1$) of contributor C_{ij}. The contribution score of the i^{th} safeguard, assuming equal consideration for each required contributor, is calculated as:

$$CS_{S_i} = \left(\frac{\sum_{j=1}^{m} C_{ij-CTR}}{m} \right) \tag{3.1}$$

The intent of equation 3.1 is to quantify the contribution-type interaction without improperly penalizing or artificially inflating any CS_i. An alternative approach for consideration would be to take the minimum C_{ij-CTR} as the contribution score for a safeguard in order to build in a "worst-case" scenario. However, this approach would inappropriately penalize a safeguard

in the overall measure of p_1. Consider the example shown in Figure 3-3, in which a standard "Access Authorization" safeguard requires contributions from people, processes, and technology. For cases in which an organization maintains paper-based access authorizations as opposed to maintaining and managing them electronically using software, the C_{ij-CTR}value for technology would be 0, resulting in contribution score of 0 for the safeguard. However, this would prevent the contribution score from capturing the fact that access authorization is occurring, albeit not in the most efficient manner. Using the contribution score presented here is more meaningful in that indicates a safeguard is supporting overall ISS confidentiality, but *at a reduced level* than that which could otherwise be achieved.

Wang and Wulf (1997) have proposed approaches such as the Weakest Length (WL), Weighted Weakest Length (WWL), and Prioritized Siblings (PS) for capturing the functional relationships among factors when estimating system security. In this case, adapting and applying these approaches would lead to selecting the minimum C_{ij-CTR} (WL), applying weight values to each contributor (PS), or a combination of both (WWL). As discussed above, these approaches would lead to inappropriately penalizing a safeguard in final the overall measurement, or would violate the established assumption of un-weighted elements in $\mathbf{C}_i$.

3.5.2.2 Dependency-Type Interaction

When dependencies exist for a S_i, specifically when there is a corresponding $\mathbf{S_iD}$, safeguard subsystem-level interactions are present. The net effect on the safeguard's contribution score is accounted for by calculating a dependency score (x_{S_i}) which incorporates the contribution scores of the safeguards on which it depends:

$$x_{s_i} = \min\left(CS_{S_i}, \frac{CS_{S_i} + \sum_{S_d \in \mathbf{S_i D}} CS_{S_d}}{1 + k}\right) \tag{3.2}$$

where:

k is the number of safeguards in $\mathbf{S_i D}$

d is the ith index of the corresponding safeguard in **S**

The score calculation shown in equation 3.2 can be viewed as the minimum of the safeguard contribution score and a modified contribution score for S_i that is calculated against the maximum contribution score possible for a *safeguard complex* (i.e. the score for S_i *and* the scores of all safeguards on which it depends). The minimum is invoked to ensure that the dependency score for a safeguard can never exceed that of its individual contribution score. Quantifying the dependency-type interactions is an important concept, as it begins to aggregate the affects of contributions across multiple dependent safeguards. For cases in which a safeguard has no dependencies, x_{S_i} is equivalent to CS_{S_i}.

3.5.2.3 Constraint-Type Interaction

As described in Section 3.4.2.1, the constraint-type interaction (contributor subsystem-level interaction) occurs among the contributor elements in $\mathbf{C_i}$, and is viewed as having a *limiting* affect on a contributor element's contributions to a safeguard. It is important to account for this type of constraint in the measurement concept as it attempts to address the affects that contributor-contributor friction can have on confidentiality.

When this type of interaction is determined to be present among one or more elements, , the first element (q=0) of $\mathbf{C_iI_q}$ represents the "constrained" element and all remaining elements (q > 0) represent the "constrained by" elements. For example, using the illustration shown in Figure 3-5, the contributor element "authorization process" is constrained by the actions of the "data owner". Therefore, if the contribution value of the data owner is less than that of the authorization process, the contribution value of the authorization process becomes the minimum of the two values:

$$C_{ij-CTI} = \min\{C_{i0-CTR}, C_{i1-CTR}, .. C_{iq-CTR}\} \tag{3.3}$$

where:

C_{ij-CTI} is the augmented contribution value for contributor *ij* (the constrained element)

$C_{i0-CTR}, C_{i1-CTR}, .. C_{iq-CTR}$ are the elements in $\mathbf{C_iI_q}$

In this case the minimum is appropriate, as a constraint-type interaction between contributor elements indicates that the maximum contribution from the constrained contributor is limited by the minimum contribution of the contributors with which it is constrained by. Constraint-type interactions are intended to capture undesirable actions in the contributor subsystem, and the ISS measure of confidentiality should reflect their existence. The illustration shown in Figure 3-9 indicates the three types interactions discussed in this section in the context of the structural formalization developed in 3.5.1.

1. Contributor subsystem contained interaction (constraint): Contributors interact, interactions affect contributions to safeguards.
2. ISS contained interaction (contribution): contributors contribute to safeguards.
3. Safeguard subsystem contained interaction (dependency): The ability of a safeguard to maintain confidentiality is affected by that of any safeguards on which it depends.

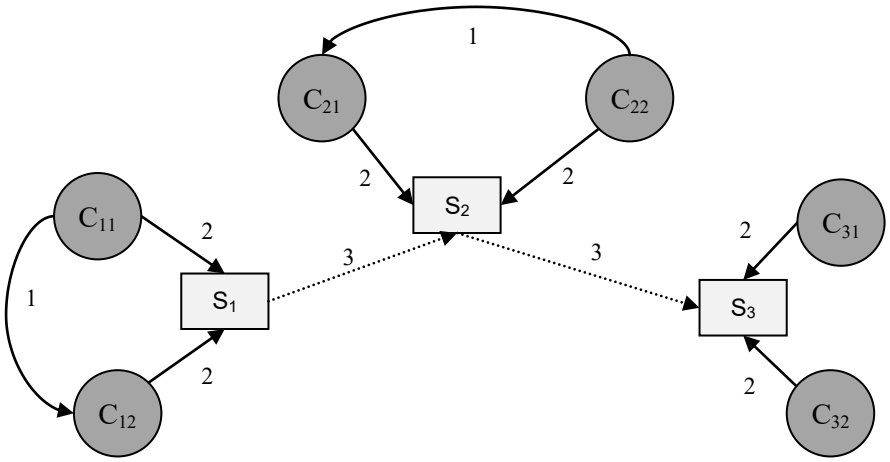


Figure 3-9 Interactions and formalized elements in the overall measurement concept

3.5.2.4 Total ISS Confidentiality (p_1)

As previously discussed, the existence of emergent properties is predicated on the interactions of contained elements (systems and subsystems) which are conceptually nested within their parent (i.e. containing) system. p_1 is considered to be an emergent property of the ISS as its calculation is based on the interactions that occur 1) among elements within the contributor subsystem, 2) among elements within the safeguard subsystem, and 3) between the elements in the contributor and safeguard subsystems.

Total ISS confidentiality is calculated by summing the products of all x_{S_i} values and their corresponding confidentiality weights, and dividing by the sum of the confidentiality weights:

$$p_1 = \frac{\sum_{i=1}^{n} w_{c_i} * x_{s_i}}{\sum_{i=1}^{n} w_{c_i}} \tag{3.4}$$

Applying a confidentiality weight (w_{c_i}) at this stage of calculation allows for the measure of p_1 to be reflect the relative importance of each safeguard with respect to confidentiality. This also permits a level of control and flexibility from the perspective of stakeholders in that they can adjust their view of information security (i.e. varying importance of safeguards with respect to confidentiality), without altering the calculations of a common underlying model.

3.5.2.5 Units and Scale

The confidentiality measurement scale is based on a minimum and maximum value of 0.00 and 1.00 for p_1, respectively. A p_1 value of 0.00 indicates the absence of any contribution from any contributor and a p_1 value of 1.00 indicates the presence of maximum contributions from all contributors. The interpretation of the scale can be viewed as follows: as the total level of safeguard contribution from people, processes, and technology increases, the measure of p_1 increases from 0.00 to 1.00. Most importantly, the measure reflects contribution values that are subject to the interactions previously defined in this section. In the next section, a metric for confidentiality is constructed using the information generated by applying the confidentiality measurement approach.

3.6 Confidentiality Metric

For an entity of which security is a meaningful concept, there is a set of attributes that characterize the security of that entity, and a security metric is a quantitative measure of how much of the attribute is possessed by the entity (SSE-CMM, 2011). In this section, the *basic definition* of a security metric as defined by the SSE-CMM is adopted and extended into a framework that complements the ISS concept developed in this chapter. Figure 3-10 shows the metrics framework which indicates the relationship among the ISS, its desired properties, and the corresponding information security metrics.

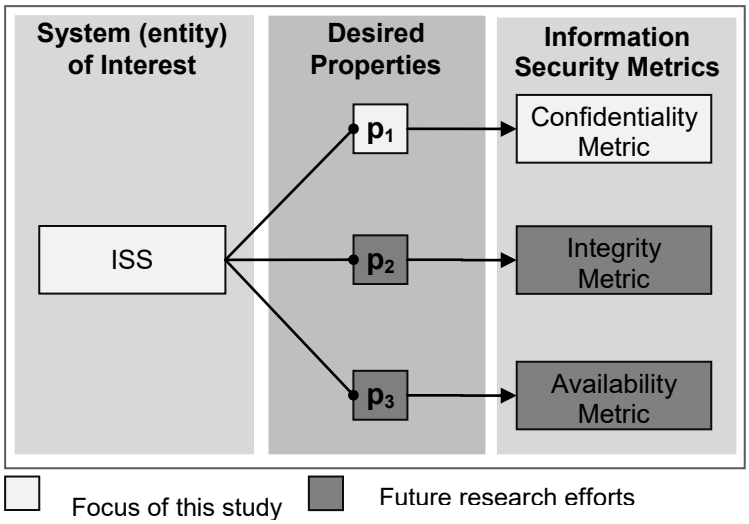


Figure 3-10 Information security metrics framework

As shown in Figure 3-10, the desired ISS properties represent the foundation for information security metrics in the proposed metrics framework. Using the p_1 measurement

approach discussed in the previous section, a confidentiality metric is constructed which provides an indicator of confidentiality within an organization's general control environment.

3.6.1 Content

The intent of the confidentiality metric is to present stakeholders with an indicator of confidentiality within the general control environment of their organization. Stakeholders need not be presented with all low-level details regarding the structure and contained interactions of an ISS. The value of the metric lies in that it is based on a measure of confidentiality derived from an underlying systemic model of information security and information confidentiality. Additionally, the metric should provide an indication of confidentiality in the context of required safeguards. Therefore, the desirable metric format should show the calculated dependency scores for each safeguard, their weighted score for confidentiality, and the final measure of p_1 calculated using this information.

3.7 Summary

In this chapter, an approach for measuring the confidentiality of electronic information in healthcare-related organizations was formulated. By adopting a systemic perspective regarding information security, a system of protection, referred to as an ISS, was synthesized and delineated from its containing organization. This was accomplished by investigating the complex, dynamic, and emergent characteristics among information security safeguards and organizational contributors, and capturing the types of structural elements and interactions that

are present. Using this information, a set of equations and rules were developed for quantifying interactions and calculating confidentiality as an emergent property of an ISS. Additionally, a metrics framework was developed which captures the relationship among the ISS, desired properties, and information security metrics. In the next chapter, an Information security model (ISM) is developed for demonstrating the measurement approach developed in this chapter.

3.7.1 Problem to Solution Traceability

In Section 3.2, four overarching requirements for a solution approach were derived. Table 3-3 provides the traceability of these attributes to their implementation in the proposed solution approach.

Table 3-3 Traceability of problem space to solution space

Solution Attribute	Solution Concept
Protection System Concept	The proposed solution delineates an ISS from the containing organizational system. This logically separates the system providing the security (ISS) from the system being secured (organization) and provides a mechanism for confidentiality measurement (i.e. as an emergent ISS property).
Delineation of Measurement	The proposed solution provides a measure of confidentiality and a corresponding metric.
Systemic Thinking	Systemic principles are the core foundation for synthesizing an ISS from the organizational problem space and for defining confidentiality as an emergent system property.
Healthcare-Specific Needs	The ISS is constructed using the HIPAA Security Rule safeguards. The proposed metric provides healthcare organizations a confidentiality metric which can be used for addressing stakeholder-specific concerns regarding the protection of personal medical information.

CHAPTER 4

INFORMATION SECURITY MODEL

In Chapter 3, an approach for measuring the confidentiality of electronic information and the supporting theoretical concepts were presented. In this chapter, an Information Security Model (ISM) is developed for implementing and demonstrating this approach. We begin by first describing the general ISM concept in Section 4.1. Then, in Section 4.2 the data to be modeled is defined and in Section 4.3, the ISM is constructed using this data.

4.1 ISM Concept Overview

The ISM is intended to provide a rigorous mechanism for specifying the nested hierarchy of systemic elements and interactions shown in Figure 3-7. Additionally, the ISM is intended to be capable of generating a measure of confidentiality using this information as discussed in Section 3.5. In this section, the concept of a *system model* which meets these criteria is described.

4.1.1 ISM Requirements

4.1.1.1 Modeling Language

A standard modeling language with strong syntax and semantics is beneficial for developing, documenting, and conveying system models. Additionally, system models developed using a standard language provide a consistent presentation and support interoperability with other similarly-developed models. It is therefore advantageous to develop

the ISM using a standard, well-established modeling language meeting these criteria. Additionally, consideration should be given to the availability of commercial software packages that provide robust modeling environments.

4.1.1.2 Simulation and Solver Capability

As discussed in Section 3.4.2 and Section 3.5.2, contained systemic interactions are a critical component of confidentiality measurement within the general control environment and subsequently the ISS. Therefore, the ISM must not only specify the interactions among information security safeguards and contributors from a qualitative perspective, but must also provide a mechanism for modeling and executing the quantitative relationships (i.e. equations) that characterize these interactions.

4.1.1.3 Model Instantiation

The ISM must be capable of being *instantiated* -- specifically, it must have the ability to accept a limited set of initial user-provided input values for the purpose of executing all quantitative relationships and generating a measure of confidentiality. Additionally, it is desirable that the mechanism for instantiation report the results of all intermediate calculations used in solving for p_1 back to the user. This data is essential for constructing a meaningful metric for confidentiality that shows not only the final measure, but also provides visibility regarding the contribution and dependency scores of safeguards.

4.1.1.4 Extensibility

Because the confidentiality of electronic information is only one view of information protection, it is desirable that the ISM be constructed to support extensibility to the remaining information security properties of the ISS identified in Section 3.4.3. Indeed, the general ISM framework should also support the inclusion of additional information-security related systems (e.g. a threat system) that may be required to address additional stakeholder concerns regarding information security.

4.1.2 Implementation

In order to address the requirements identified in Section 4.1.1, the Object Management Group (OMG) Systems Modeling Language (SysML™) was selected for developing the ISM. SysML is a general-purpose visual modeling *language* for systems engineering that provides standard constructs and diagrams for specifying and analyzing a diverse range of complex system types, such as organizational systems and those composed of people, processes, and technologies. SysML re-uses the foundations established by the Unified Modeling Language 2 (UML 2), OMG's widely-used visual modeling language for software intensive systems, and extends it to address the specific needs of systems engineering. In addition to a rigorous hierarchical structural modeling capability, SysML provides a parametric diagramming capability for modeling the relationships among quantitative system properties. Using external solving tools, it is possible to execute complex systems of equations defined using SysML parametric diagrams therefore bridging the gap between design and analysis models.

4.1.2.1 Software

The following software packages were selected for constructing and instantiating the ISM. These packages consist of a SysML modeling environment and the additional software components necessary for executing SysML parametric diagrams and solving systems of equations. Each software package is described below:

- Artisan Studio® Version 7.2.23: A commercially-available, enterprise-grade tool suite for building systems and software models using OMG SysML and UML. Upon inquiry, a fully-functional version of this software was provided for use in this study (60-day temporary license) by the vendor, Atego™. Artisan Studio® provides a SysML modeling environment and represents the primary application used for constructing the ISM.
- Artisan Studio® ParaSolver™ Version 7.2 R1: Plug-in software for executing SysML parametric diagrams developed using Artisan Studio®. ParaSolver™ provides an interface between SysML models constructed using Artisan Studio® and external solver engines. It parses structure, parametric, and instance data specified in the ISM to the external solver and provides an application browser for solving and viewing results. Upon inquiry, a fully-functional version of this software was provided for use in this study (60-day temporary license) by the vendor, Atego™.
- Wolfram Mathematica® Version 8.0: Industrial-grade computational software and a core solver utilized by ParaSolver. This application is used for solving the system of equations defined using SysML parametric diagrams. A fully-functional version of this software was acquired on a 15-day trial license from the vendor website. ParaSolver also supports the use of OpenModelica, an open-source simulation environment based on the Modelica

language, as a core solver. As part of this study, both core solvers were evaluated and the decision to use Wolfram Mathematica was predicated by the observation of OpenModelica application errors (i.e. internal class casting errors) that were generated during some model instantiations. It is noted that these errors were not generated by Mathematica during executions of the same model.

4.1.3 ISM Construction and Usage

As discussed earlier in this section, the intent of the ISM is to specify an ISS and generate a measure of confidentiality through model instantiation. The following steps encapsulate this concept:

1) Define the domain data to be modeled. Domain data consists of the HIPAA Security Rule Safeguards, the associated people, process, and technology contributors, and all associated interactions. The set of domain is generated by expanding the general types of systemic elements and interaction identified in Table 3-1 and Table 3-2.
2) Construct the ISM. The ISM is consists of two sub-models: a structure (or schema) model and an instance model. The structure model defines the basic structural components, properties, and associations of an ISS in addition to the parametric relationships among system properties. The instance model defines a specific *instance* of the structure model which contains *slots* for holding user-provided and calculated values for quantitative properties defined in the structure model.

3) Instantiate the ISM by providing a set of input contribution values and safeguard confidentiality weights, and solving for p_1 using ParaSolver. Figure 4-1 provides a context figure of the ISM concept.

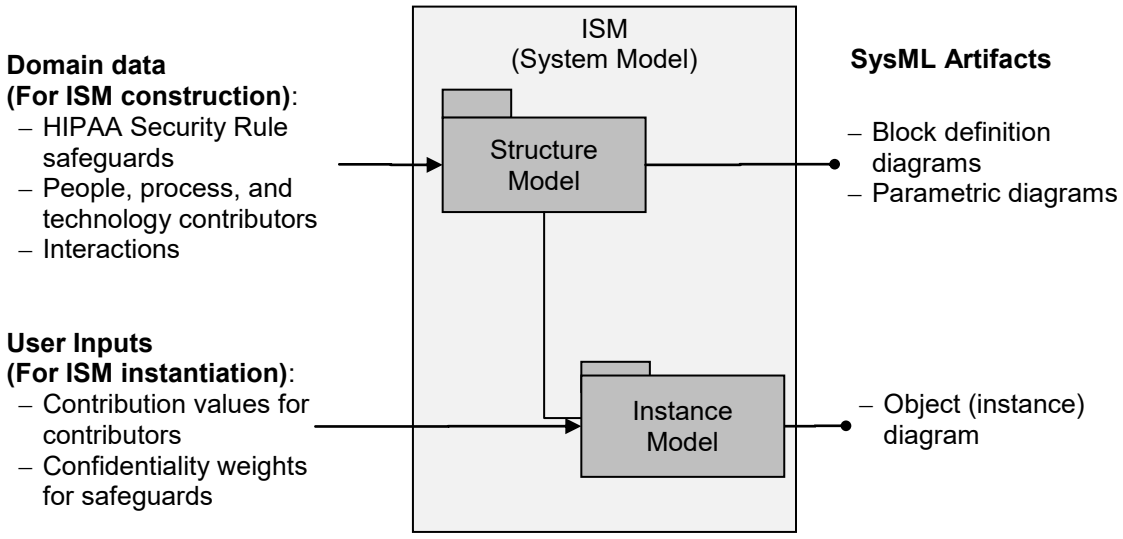


Figure 4-1 ISM concept overview

4.2 Domain Data

This section documents the domain data to be modeled in the ISM. Specifically, the HIPAA Security Rule safeguards, their respective people, process, and technology contributors, and all associated interactions are identified. This data is the result of expanding the general types of elements and interactions identified in Table 3-1 and Table 3-2. What is referred to here as domain data differs from user-input data in that domain data is used for model construction, whereas user-input data is used for model instantiation.

4.2.1 Contributors

4.2.1.1 Nomenclature

A global set of 46 information security contributors consisting of the *common* people, process, and technology elements found in practice was identified. The global contributor set is intended to be representative of the common contributors required by a set of information security safeguards. Each contributor was assigned an identifier consisting of the following format: *C- <type>-<#>*, where *C* indicates the systemic element type, in this case, a contributor, *type* indicates the general type of contributor, with "Pe", "Pr", and "Te" indicating people, process, and technology contributors, respectively and *#* represents a two-digit numeric index assigned to each contributor for a given a type. Identifiers were used to provide a consistent and efficient way for referencing each contributor element. The list of global contributors is shown in Table 4-1.

4.2.2 Safeguards

4.2.2.1 Nomenclature

Each of the 36 HIPAA Security Rule safeguards shown in Table 2-1 were assigned a unique identifier consisting of the following format: *S-<type>-<#>*, where *S* indicates the systemic element type, in this case a safeguard, *type* indicates the type of safeguard as identified by the HIPAA Security Rule, with "Adm", "Phy", and "Tec" indicating administrative, physical, and technical safeguards, respectively and *#* represents a two-digit numeric index assigned to each safeguard for a given a type. Like contributors, identifiers were used to provide a consistent

and efficient way for referencing each safeguard element within the ISM. Each safeguard and its respective identifier can be seen in the left-most column of Table 4-2.

Table 4-1 Global contributor data

Contributor Element	Type	ID	Contributor Element	Type	ID
Organizational management	People	C-Pe-01	Training & refresher process	Process	C-Pr-11
IT security management	People	C-Pe-02	Antivirus signature update process	Process	C-Pr-12
Human resources	People	C-Pe-03	Password maintenance procedures	Process	C-Pr-13
Data owner	People	C-Pe-04	Incident response procedures	Process	C-Pr-14
System administrator	People	C-Pe-05	Testing and revision process	Process	C-Pr-15
Application administrator	People	C-Pe-06	Criticality ranking process	Process	C-Pr-16
Application owner	People	C-Pe-07	Physical access process	Process	C-Pr-17
Contracts management	People	C-Pe-08	Maintenance process	Process	C-Pr-18
System users	People	C-Pe-09	Disposal & sanitization process	Process	C-Pr-19
Application users	People	C-Pe-10	I&A process	Process	C-Pr-20
Facilities management	People	C-Pe-11	Emergency access process	Process	C-Pr-21
Facility security	People	C-Pe-12	Backup and storage process	Process	C-Pr-22
Operations management	People	C-Pe-13	Resource accountability process	Process	C-Pr-23
Risk analysis process	Process	C-Pr-01	Risk analysis software	Technology	C-Te-01
Risk management plan	Process	C-Pr-02	Authorization tracking software	Technology	C-Te-02
Sanction process	Process	C-Pr-03	Audit reduction software	Technology	C-Te-03
Account review process	Process	C-Pr-04	Security training software	Technology	C-Te-04
Access Authorization process	Process	C-Pr-05	Antivirus software	Technology	C-Te-05
Termination procedures	Process	C-Pr-06	System software	Technology	C-Te-06
External business processes	Process	C-Pr-07	Application software	Technology	C-Te-07
Access establishment process	Process	C-Pr-08	Backup software	Technology	C-Te-08
Access modification process	Process	C-Pr-09	Property tracking software	Technology	C-Te-09
Access removal process	Process	C-Pr-10	Sanitization tools/software	Technology	C-Te-10

4.2.3 Interactions

4.2.3.1 Dependency-Type

While safeguards are documented in information security standards, the interactions (i.e. dependencies) that are present among them must be determined. As discussed in Chapter 3,

safeguard-to-safeguard interactions are dependency-type relationships present within the general control environment, indicating that the efficacy of a specific safeguard is affected by the efficacy of any safeguard on which it depends. For this study, the interactions among safeguards were identified by first determining the definition, purpose, and intent of each safeguard. Because the definition of a specific safeguard can vary across information security standards, the guidance provided in NIST SP 800-66 *An Introductory Resource for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (NIST, 2008) was leveraged for clarification of safeguard definitions with respect to the HIPAA Security Rule. Next, this knowledge, along with the authors experience in evaluating information security safeguards in practice, was used for determining the dependencies among each safeguard. Although the dependencies are relative to the HIPAA Security Rule safeguards, they are generally representative of those that would exist among the common safeguards of other information security standards and problem domains.

4.2.3.2 Contribution Type

Each safeguard element requires a set of contributors and contributions. The set of contributors for each safeguard is a subset of the global information security contributor list and there is no restriction on the number of safeguards that any individual contributor can contribute to (i.e. one-to-many relationship may be present among a contributor and safeguard element).

4.2.3.3 Constraint Type

Among the set of contributor elements for each safeguard, there are zero or more constraint interactions. Note that it is not necessarily the case a constraint type interaction will be associated with each safeguard. The intent was to identify common types of constraint relationships seen in practice, specifically regarding confidentiality-focused safeguards.

Table 4-2 identifies all interactions among safeguards and contributors. The data displayed in Table 4-2 should be interpreted in the following manner:

- An element in the Safeguard column *depends on* the corresponding safeguard elements identified in the Dependency Interaction column.
- The elements in the Contribution Interaction column *contribute to* the corresponding element in the Safeguard column.
- The elements in the Constraint Interaction column constrain or are constrained by one another as indicated.

Table 4-2 Safeguard and contributor interaction matrix

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Risk Analysis S-Adm-01	N/A	C-Pe-01: Contributes Top-level support C-Pe-02: Contributes Implementation of risk analysis C-Pr-01: Contributes Policy for risk analysis	C-Pe-02 is constrained by C-Pe-01
Risk Management S-Adm-02	S-Adm-01: Risk management requires the results of risk analysis in order to adequately mitigate risks to the confidentiality of EPHI.	C-Pe-01: Contributes Top-level support C-Pe-02: Contributes Implementation of mitigation approach C-Pr-02: Contributes Mitigation approach C-Te-01: Contributes Risk tracking	C-Pe-02 is constrained by C-Pe-01
Sanction Policy S-Adm-03	S-Adm-04: Sanction policy cannot be applied unless suspicious actions performed by individuals have been identified via information system activity reviews. S-Adm-13: Sanction policy cannot be applied unless suspicious activities have been identified via audit data captured through log-in monitoring.	C-Pe-03: Contributes Implementation of sanction policy C-Pe-04: Contributes Notification of unauthorized activity C-Pe-07: Contributes Notification of unauthorized activity C-Pr-03: Contributes Sanction policy C-Te-02: Contributes Authorization artifacts	N/A

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Information System Activity Review S-Adm-04	S-Tec-01: Information system activity reviews require unique user identifiers for EPHI applications and information systems in order to establish accountability for information system activity	C-Pe-05: Contributes Implementation of review policy C-Pe-06: Contributes Implementation of review policy C-Pe-07: Contributes Implementation of review policy C-Pr-04: Contributes Policy for review of information system accounts C-Te-06: Contributes Audit data C-Te-07: Contributes Audit data C-Te-03: Contributes Audit review capability	C-Pr-04 is constrained by C-Te-03
Authorization and/or Supervision S-Adm-05	S-Adm-09: Authorization and supervision of the workforce requires that individuals be authorized and approved for access to EPHI.	C-Pe-04: Contributes Access approvals C-Pe-06: Contributes Access approvals C-Pr-05: Contributes Policy for authorization of EPHI access C-Te-02: Contributes Authorization artifacts	C-Pr-05 is constrained by C-Pe-04 and C-Pe-06

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Workforce Clearance Procedure S-Adm-06	S-Adm-09: Workforce clearance requires a process for authorizing access to EPHI. S-Adm-07: Workforce clearance requires a process for removing access to EPHI. S-Adm-10: Workforce clearance requires an approach for granting/terminating user access to EPHI.	C-Pe-03: Contributes Implementation of workforce clearance process C-Pr-05: Contributes Policy for authorization of EPHI access C-Te-02: Contributes Authorization artifacts	C-Pr-05 is constrained by C-Pe-03
Termination Procedures S-Adm-07	S-Adm-09: In order for the accesses of terminated employees to be removed, it must be known that these accesses exist. S-Tec-01: Unique user identifiers support the removal of individual accesses upon employee termination/separation.	C-Pe-03: Contributes Notification of termination C-Pe-07: Contributes Implementation of termination policy C-Pe-06: Contributes Implementation of termination policy C-Pe-04: Contributes Notification of termination C-Pr-06: Contributes Policy for termination C-Te-02: Contributes Authorization artifacts	C-Pe-06 is constrained C-Pe-03
Isolating Health care Clearinghouse Function S-Adm-08	S-Adm-21: Requires written contract or other documented arrangements regarding how external agencies (e.g. data center hosting, data backup services) protect EPHI from unauthorized disclosure.	C-Pe-02: Contributes Implementation of policy C-Pe-04: Contributes Implementation of policy C-Pr-07: Contributes Policy for external business partners	C-Pr-07 is constrained by C-Pe-02 and C-Pe-04

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Access Authorization S-Adm-09	N/A	C-Pe-04: Contributes Approval/disapproval of access requests for EPHI applications C-Pe-07: Contributes Approval/disapproval of access requests for EPHI applications C-Pr-05: Contributes Policy for access approval C-Te-02: Contributes Authorization artifacts	C-Pr-05 is constrained by C-Pe-04 and C-Pe-07
Access Establishment and Modification S-Adm-10	S-Adm-09: The establishment and modification of user accesses requires formal authorization and approvals.	C-Pe-05: Contributes Implementation of access policy C-Pe-06: Contributes Implementation of access policy C-Pr-08: Contributes Policy for access establishment C-Pr-09: Contributes Policy for access modification C-Pr-10: Contributes Policy for access removal C-Te-02: Contributes Authorization artifacts	C-Pr-08 is constrained by C-Pe-06

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Security Reminders S-Adm-11	N/A	C-Pe-09: Contributes Acceptance of responsibility C-Pe-10: Contributes Acceptance of responsibility C-Pe-02: Contributes Implementation of training/refresher policy C-Pr-11: Contributes Training/refresher policy C-Te-04: Contributes Capability for security reminders	N/A
Protection from Malicious Software S-Adm-12	N/A	C-Pe-09: Contributes Acceptance of responsibility C-Pe-10: Contributes Acceptance of responsibility C-Pr-12: Contributes Virus signature update policy C-Te-05 : Contributes Policy regarding malicious software protection	C-Te-05 is constrained C-Pr-12

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Log-in Monitoring S-Adm-13	S-Tec-01: In order for login monitoring to provide meaningful data, unique identifiers must be utilized. Otherwise, accountability cannot be established and log-in monitoring provides no meaningful indicators for who has accessed EPHI applications.	C-Pe-04: Contributes Implementation of review policy C-Pe-05: Contributes Implementation of review policy C-Pe-06: Contributes Implementation of review policy C-Pe-07: Contributes Implementation of review policy C-Pr-04: Contributes Account review policy C-Te-03: Contributes Audit data C-Te-06: Contributes Audit data C-Te-07: Contributes Audit review capability	C-Pr-04 is constrained by C-Pe-04, C-Pe-05, C-Pe-06, and C-Pe-07
Password Management S-Adm-14	S-Adm-11: Effective password management requires the use of security reminders which informs users of the acceptable use of passwords, password complexity requirements, aging, etc.	C-Pr-13: Contributes Password policies C-Te-06: Contributes Password settings C-Te-07: Contributes Password settings C-Pe-05: Contributes Implementation of password policy C-Pe-06: Contributes Implementation of password policy	C-Pr-13 is constrained by C-Pe-05 and C-Pe-06

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Response and Reporting S-Adm-15	S-Adm-04: Response and reporting requires the identification of potentially suspicious actions regarding EPHI detected through information system activity reviews. S-Adm-13: Response and reporting requires the results of log-in monitoring to identify reportable incidents such as unauthorized attempts to access EPHI. S-Adm-12: Response and reporting requires the results of antivirus/antispyware scans (i.e. malicious software protection) to identify reportable incidents.	C-Pr-14: Contributes Incident response policy C-Pe-09: Contributes Notification of incident C-Pe-10: Contributes Notification of incident C-Pe-05: Contributes Reporting of incidents C-Pe-06: Contributes Reporting of incidents	C-Pr-14 is constrained by C-Pe-05 and C-Pe-06
Data Backup Plan S-Adm-16	S-Adm-20: Data backup plan requires criticality ranking of applications to determine application and data backup schedule.	C-Pe-13: Contributes Implementation of data backup plan C-Pr-22: Contributes Backup and storage policy C-Te-08: Contributes Backup capability	

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Disaster Recovery Plan S-Adm-17	S-Adm-16: Requires a data backup plan – if data is not backed up, it cannot be restored during a disaster recovery scenario. S-Adm-20: Requires a list of critical applications for prioritization of EPHI application/data recovery during a disaster recovery scenario. S-Adm-19: Requires incorporation of testing and revision results in order to address deficiencies identified during testing. S-Phy-01: Requires procedures and controls for access to EPHI during the execution of emergency operations.	C-Pe-13: Contributes Disaster recovery plan input C-Pe-11: Contributes Disaster recovery plan input C-Pe-02: Contributes Disaster recovery plan input	
Emergency Mode Operation Plan S-Adm-18	S-Adm-19: Requires incorporation of testing and revision results in order to address deficiencies identified during testing. S-Adm-16: Requires a data backup plan – if data is not backed up, it cannot be restored during an emergency mode/business continuity scenario. S-Phy-01: Requires procedures and controls for access to EPHI during the execution of the emergency operations mode (business continuity) plan	C-Pe-13: Contributes EMO plan input C-Pe-11: Contributes EMO plan input C-Pe-05: Contributes EMO plan input C-Pe-06: Contributes EMO plan input	

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Testing and Revision Procedure S-Adm-19	N/A	C-Pe-13: Contributes Execution of plan testing and revision C-Pe-11: Contributes Execution of plan testing and revision C-Pe-02: Contributes Execution of plan testing and revision C-Pe-05: Contributes Execution of plan testing and revision C-Pe-06: Contributes Execution of plan testing and revision C-Pr-15: Contributes Execution of plan testing and revision	
Applications and Data Criticality Analysis S-Adm-20	N/A	C-Pe-04: Contributes Ranking of data (process implementation) C-Pe-02: Contributes Ranking of application (process implementation) C-Pr-16: Contributes Data and application criticality ranking policy	

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Written Contract or Other Arrangement S-Adm-21	S-Adm-16: Written contracts or other formal documented arrangements establish the expected level of service from external agencies regarding how they backup EPHI applications. S-Adm-17: Written contracts or other formal documented arrangements establish the expected level of service from external agencies regarding how they recover EPHI applications in a disaster recovery scenario. S-Adm-18: Written contracts or other formal documented arrangements establish the expected level of service from external agencies regarding how they protect EPHI during an emergency mode/business continuity scenario. S-Adm-19: Written contracts or other formal documented arrangements establish the expected level of service from external agencies regarding how they test associated plans	C-Pe-02: Contributes Implementation of policy C-Pe-08: Contributes Service level agreements C-Pr-07: Contributes Policy for external business partners	

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Contingency Operations S-Phy-01	N/A	C-Pe-11: Contributes Implementation of contingency operations C-Pe-12: Contributes Implementation of contingency operations C-Pe-13: Contributes Implementation of contingency operations C-Pe-01: Contributes Implementation of contingency operations	
Facility Security Plan S-Phy-02	S-Adm-01: Requires that risks to the physical location of the facility and the facility itself be determined and addressed in the plan. S-Phy-04: Requires maintenance records associated with host facility (where EPHI is stored/transmitted/processed) and associated physical inventory. S-Phy-01: Requires procedures and controls for access to EPHI during the execution of the execution of contingency operations.	C-Pe-11: Contributes Facility security plan input C-Pe-12: Contributes Facility security plan input	

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Access Control and Validation Procedures S-Phy-03	S-Adm-10: The establishment and modification of user accesses provides the approach for establishing and modifying physical access to locations where EPHI is stored, transmitted, and received. S-Adm-09: Physical access control and validation of physical access requires that an individual's access to areas where EPHI is stored, maintained, or transmitted be authorized, or formally approved and documented.	C-Pe-12: Contributes Implementation of access control and validation policy C-Pr-17: Contributes Policy for physical access validation C-Te-02: Contributes Authorization artifacts	
Maintenance Records S-Phy-04	N/A	C-Pe-11: Contributes Implementation of maintenance policy C-Pe-12: Contributes Implementation of maintenance policy C-Te-09: Contributes Property tracking artifacts C-Pr-18: Contributes Maintenance policy C-Pr-19: Contributes Policy for facilities maintenance	

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Disposal S-Phy-05	N/A	C-Pe-11: Contributes Implementation of policy C-Pe-12: Contributes Implementation of policy C-Pr-19: Contributes Policy for disposal and sanitization C-Te-09: Contributes Property tracking artifacts C-Te-10: Contributes Disposal and sanitization capability	C-Pr-19 is constrained by C-Pe-11 and C-Pe-12
Media Re-use S-Phy-06	S-Phy-05: Requires a means for disposing or sanitizing media of EPHI prior to issuance for re-use.	C-Pr-19: Contributes Disposal and sanitization policy C-Pe-05: Contributes Implementation of media-reuse policy C-Pe-02: Contributes Implementation of media-reuse policy C-Te-09: Contributes Property tracking artifacts C-Te-10: Contributes Disposal and sanitization capability	C-Pr-19 is constrained by C-Pe-05 and C-Pe-02
Accountability S-Phy-07	S-Phy-05: Accountability for hardware and software requires an approach for disposal (which includes the identification of hardware/software maintained by the organization).	C-Pe-02: Contributes Implementation of accountability policy C-Pe-11: Contributes Implementation of accountability policy C-Te-09: Contributes Property tracking artifacts C-Pr-23: Contributes Policy for accountability	C-Pr-23 is constrained by C-Pe-11

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Data Backup and Storage S-Phy-08	S-Adm-16: Requires a backup approach (schedule/frequency/etc.) for EPHI data and applications.	C-Pe-13: Contributes Implementation of backup and storage policy C-Pr-22: Contributes Backup and storage policy C-Te-08: Contributes Backup and storage	N/A
Unique User Identification S-Tec-01	N/A	C-Pr-20: Contributes Identification and authentication policy C-Te-06: Contributes Authenticator management capability C-Te-07: Contributes Authenticator management capability C-Pe-02: Contributes Implementation of identification and authentication policy	C-Pr-20 is constrained by C-Te-06 and C-Te-07
Emergency Access Procedure S-Tec-02	N/A	C-Pe-02: Contributes Implementation of emergency access policy C-Pr-21: Contributes Emergency access policy	N/A
Automatic Logoff S-Tec-03	N/A	C-Pe-02: Contributes Implementation of log-off capability C-Te-06: Contributes Automatic log-off capability C-Te-07: Contributes Automatic log-off capability	C-Pe-02 is constrained by C-Te-06 and C-Te-07

Safeguard	Dependency Interaction (Safeguard-Safeguard)	Contribution Interaction (Contributor-Safeguard)	Constraint Interaction (Contributor-Contributor)
Encryption and Decryption S-Tec-04	N/A	C-Pe-02: Contributes Implementation of encryption/decryption capability C-Te-06: Contributes Data encryption capability C-Te-07: Contributes Data encryption capability	N/A
Mechanism to Authenticate Electronic Protected Health Information S-Tec-05	S-Tec-06: Requires that controls be in place for authenticating EPHI data (i.e. determining that it has not been altered or destroyed in an unauthorized manner).	C-Pe-02: Contributes Implementation of authentication mechanisms for EPHI C-Te-06: Contributes Encryption capability C-Te-07: Contributes Encryption capability	C-Pe-02 is constrained by C-Te-06 and C-Te-07
Integrity Controls S-Tec-06	S-Tec-07: An approach for protecting EPHI from unauthorized modification during transmission requires the use of encryption mechanisms. S-Tec-04: An approach for protecting EPHI from unauthorized modification during transmission requires the use of encryption and decryption mechanisms.	C-Pe-02: Contributes Implementation of integrity capability C-Te-06: Contributes Data integrity C-Te-07: Contributes Data integrity	N/A
Encryption S-Tec-07	N/A	C-Pe-02: Contributes Implementation of encryption capability C-Te-06: Contributes Data encryption C-Te-07: Contributes Data encryption	C-Pe-02 is constrained by C-Te-06 and C-Te-07

4.3 ISM Structure Model

In this section, the domain data presented in the previous section is modeled using SysML block definition and parametric diagrams. This collection of diagrams represents the ISM structure model.

4.3.1 Block Definition Diagrams

Block definition diagrams are the primary SysML structural diagram type and are used for defining the properties and relationships of blocks. This section provides a brief description of blocks and properties, and presents the block definition diagrams of the ISM.

4.3.1.1 Blocks

Blocks are the fundamental structural elements used in SysML modeling. They provide a general-purpose modeling capability that can be used to represent a diverse range of real-world objects and concepts. Blocks are characterized in terms of their properties, which further define their features and relationships with other blocks. Value properties, part properties, and constraint properties are of primary interest in constructing the ISM as they are essential for generating a structure model that can be instantiated and solved using ParaSolver. Each property type and its role in the ISM are briefly described below.

4.3.1.1.1 Value properties

Value properties represent quantitative characteristics that describe a block. In the ISM, value properties are used to define values used in the quantification of interactions among

contributors and safeguards (e.g. contribution and dependency scores) and in the measure of confidentiality within the ISS. All value properties defined in the ISM are of the type "Real", indicating they are represented by a real number.

4.3.1.1.2 Part Properties

Part properties indicate a composite relationship among blocks and are defined using *associations*. In the ISM, the *composition* association is used, as it implies a whole-part relationship among the connected blocks, indicating the existence of any hierarchical level is predicated on that of its parent.

4.3.1.1.3 Constraint Properties

Constraint properties indicate the existence of a *constraint* on the value properties of a block. Constraint properties are themselves defined using *constraint blocks*, a special type of SysML block which contains equations that relate the value properties of one or more blocks. Like part properties, constraint properties are defined for a block using the composition association between the owning block and the constraint block. In the ISM, constraint properties are the primary mechanism for modeling the quantitative relationships that characterize systemic interactions and the calculation of confidentiality.

4.3.1.2 ISM Block Definition Diagrams

As discussed in Section 3.4.3, the ISS consists of a hierarchy of systems, subsystems, and elements which reside within the containing organizational system. Figure 4-2 provides a block definition diagram that defines the top three levels of the hierarchy.

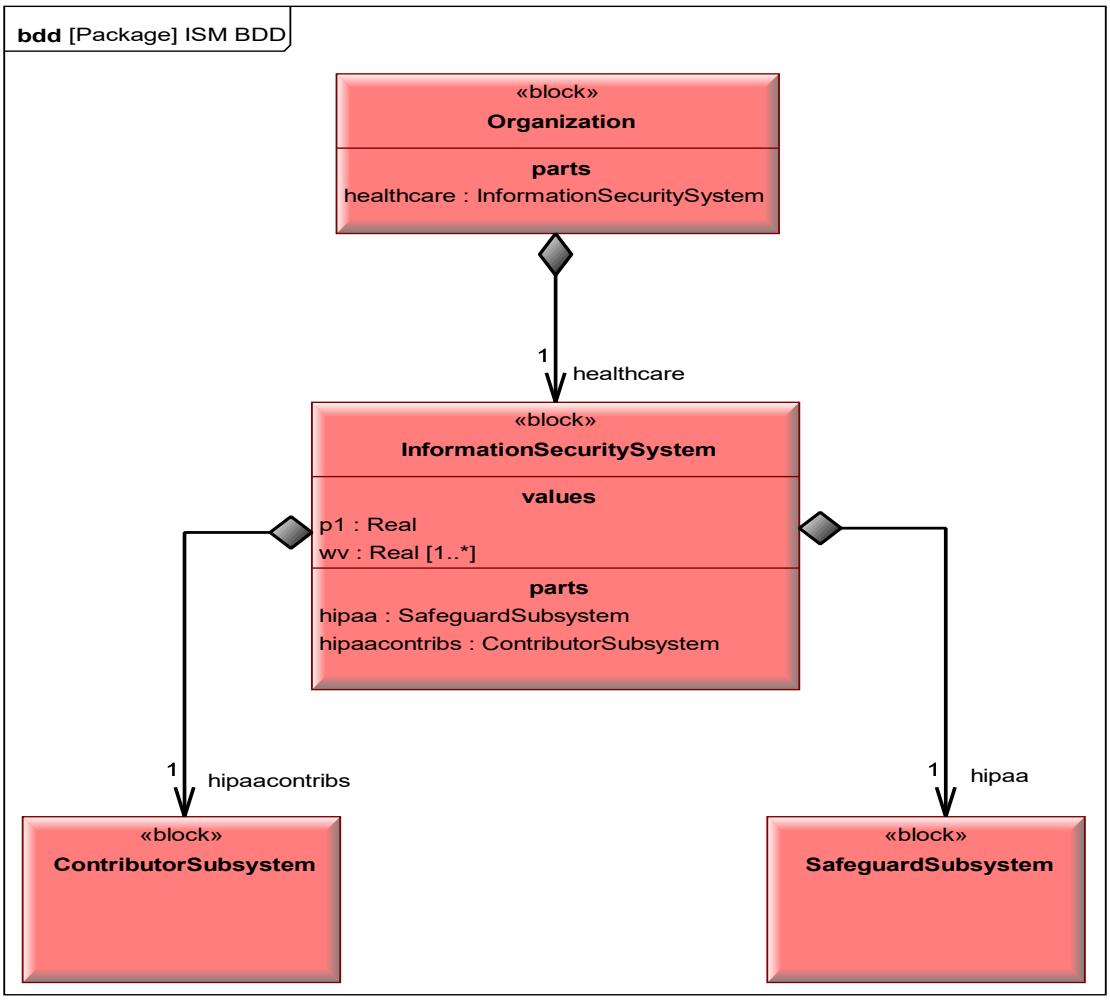


Figure 4-2 ISM block definition diagram

In Figure 4-2, the systemic hierarchy of blocks is defined using the composition association implying a whole-part relationship among the organization, system, and subsystem levels. This results in part properties for the organization and information security system blocks (shown in the "parts" compartment of the respective block). For example, the information security system is composed of safeguard and contributor subsystems which are defined by the

part properties *hipaa* and *hipaacontribs*, respectively. Additionally, the multiplicity of each association is strictly set to 1, indicating that *only one* information security system, consisting of *only one* safeguard subsystem and *only one* contributor subsystem, exists within an organization.

Also illustrated in Figure 4-2 are the block value properties that are necessary for developing parametric diagrams and instantiating the ISM. The information security system block contains two value properties (shown in the "values" block compartment), one which represents the overall measure of confidentiality (p_1) and one which represents the safeguard confidentiality weights (*wv*). Note that the latter is defined as an *aggregate* value property as indicated by its multiplicity of [1…*]. An aggregate value property is similar to array of real numbers and in this case is advantageous as it eliminates the need for 36 additional value properties necessary for individually representing each safeguard confidentiality weight in the model.

Not shown in Figure 4-2 (for readability purposes) is the lowest level of the systemic hierarchy consisting of the safeguard and contributor elements that compose the safeguard and contributor subsystems, respectively. Two additional block definition diagrams were created to capture each subsystem and their associations with the elements of which they are composed. Figure 4-3 and Figure 4-4 provide block definition diagrams for the safeguard and contributor subsystems, respectively.

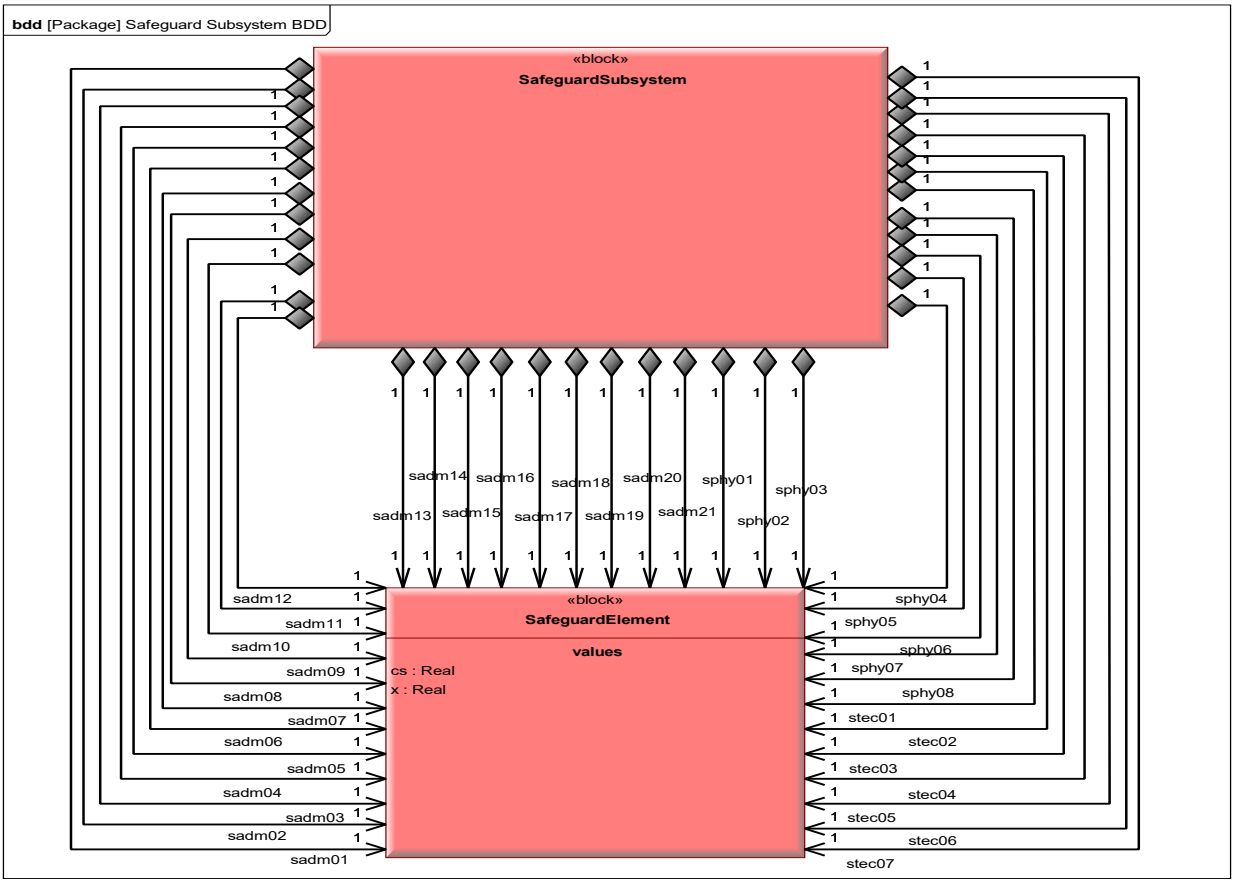


Figure 4-3 Safeguard subsystem block definition diagram

Figure 4-3 indicates two value properties for a safeguard element, one which represents its contribution score (*cs*) and one which represents its dependency score (*x*). The composition association was used to define 36 individual part properties for the safeguard subsystem, each representing a safeguard element and named according to the nomenclature scheme developed in Section 4.2. In SysML, it is possible to define a composite or *aggregate part property* which, in this case, would indicate that a safeguard subsystem may contain an arbitrary number of

safeguard elements (for example, a single aggregate part property *element* with a multiplicity of 1…* could be defined using an association between the safeguard subsystem and safeguard element blocks) . This is not appropriate for the ISM as the safeguard elements are not arbitrary parts, but will indeed be defined in terms of their own interactions. Explicitly defining each safeguard element using unique part properties is also necessary for instantiation.

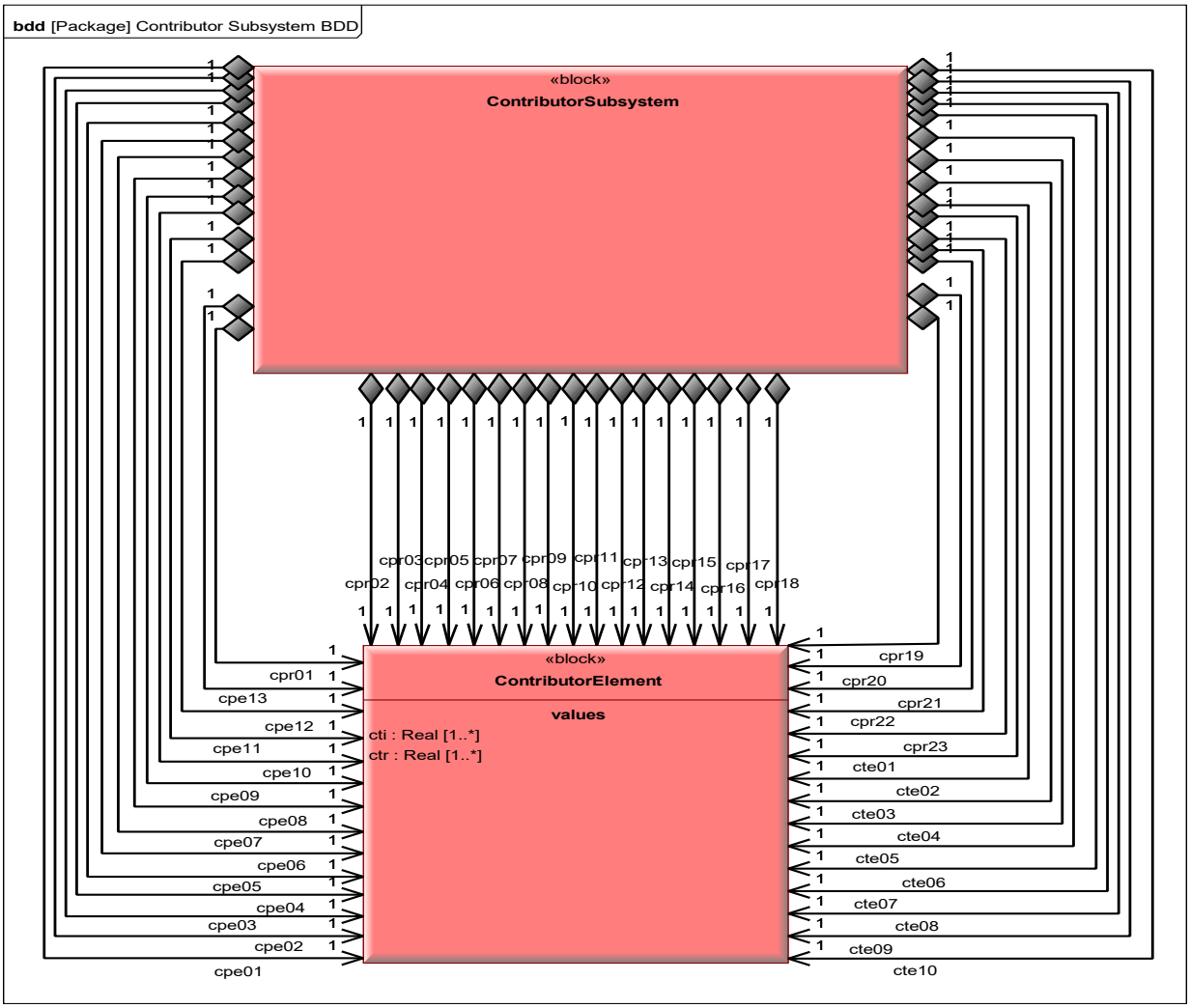


Figure 4-4 Contributor subsystem block definition diagram

Figure 4-4 provides a block definition diagram of the contributor subsystem and its associations with the contributor element block. 46 part properties were defined for the contributor system consistent with the 46 individual contributors identified in Table 4-1. Two aggregate value properties were defined for the contributor element block. Because any contributor can interact with (i.e. contribute to) more than one safeguard element, it was necessary to use an aggregate value property for the contribution value (*ctr*). The aggregate value property in this case holds the indexed *ctr* values corresponding to the safeguards with which it interacts. Similarly because a contributor can participate in more than one constraint-type interaction, an aggregate value property was required for the augmented contribution score (*cti*).

4.3.1.3 Interactions

The three types of systemic interactions identified in Table 3-2 were modeled using three general types of constraints blocks that are associated with the system or subsystem in which the interaction occurs. This was accomplished using composition associations, creating constraint properties for each owning block. Each constraint type and it's representation within the ISM is discussed in the following subsections. Note: SysML refers to constraint block equations as *constraints* as they are viewed as mechanisms for constraining the values of system properties in support of analysis efforts. This point is made to avoid confusion, as in this study a "constraint-type" interaction has been defined as a contributor subsystem-level interaction between one or more contributor elements

4.3.1.3.1 ISS (Contribution-Type) Constraint Blocks

The purpose of a contribution-type constraint block is to define the contribution score (*cs)* calculation shown in equation 3.1 for each safeguard. As previously discussed, the underlying measurement theory necessitates the use of aggregate value properties for *ctr* and *cti*. Because of this structure, and the manner in which indexed values from aggregate value properties are used, a *unique* contribution-type constraint block was required for each safeguard due to the nature of the one-to-many relationship between contributor and safeguard elements. Figure 4-5 provides a block definition diagram of the ISS-level contribution-type constraint blocks, with two constrain blocks magnified to illustrate the form of the contained equations.

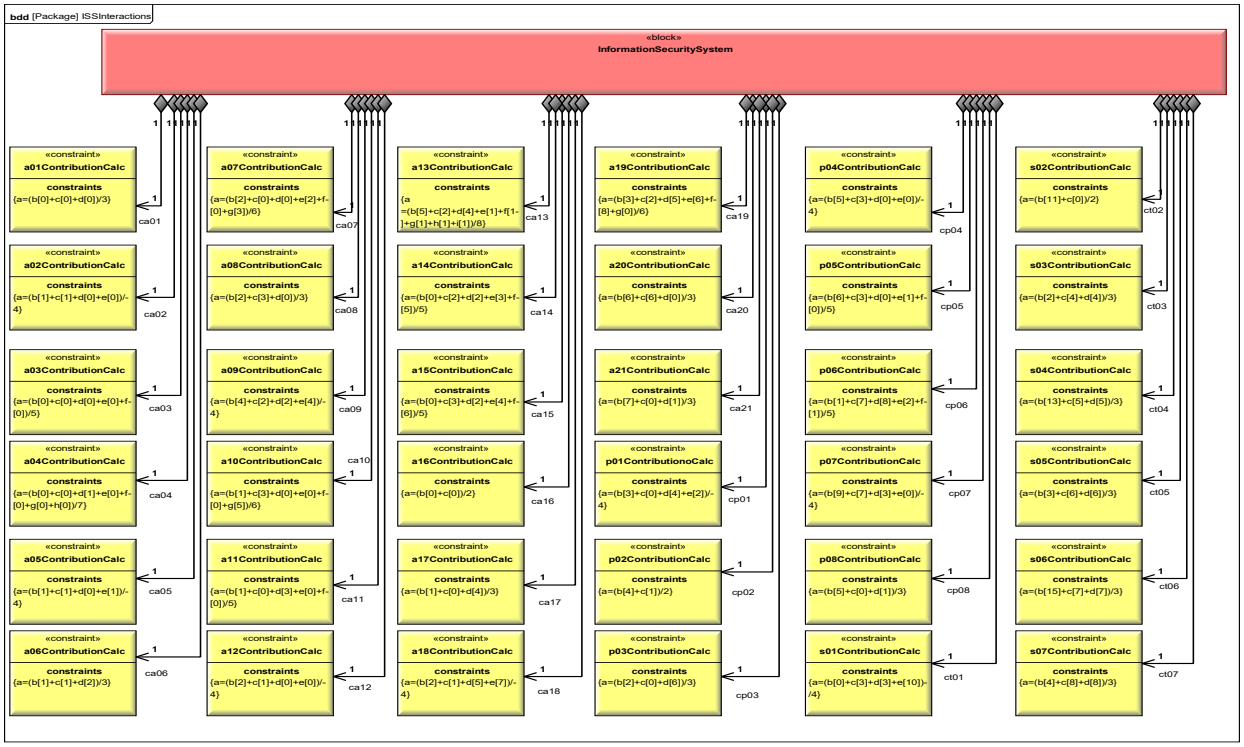


Figure 4-5 ISS system-level interactions block definition diagram

The information security system block owns 36 contribution-type constraint blocks which corresponds to 36 unique constraint properties. The manner in which value properties are connected to the parameters defined in each constraint block equation, a concept referred to as *binding*, will be further detailed in Section 4.3.2 as part of the discussion of ISM parametric diagrams.

4.3.1.3.2 Safeguard Subsystem (Dependency-Type) Constraint Blocks

The purpose of dependency-type constraint blocks is to define the dependency score calculation shown in equation 3.2 for each safeguard element. Unlike the case of contribution-type constraint blocks, unique dependency-type constraint blocks are not necessary for each safeguard element because aggregate value properties are not used in the equations for calculating x (i.e. varying index values do not need to be accounted for). 5 generic constraint blocks were defined for the cases of k0, k1, k2, k3, and k4 constraints, where k indicates the number of dependencies for a given safeguard.

Using the composition association, each block is appropriately *re-used* in order to create the necessary 36 constraint properties for the safeguard subsystem. Note that for cases in which a safeguard has no dependencies, the corresponding k0 constraint is an equality relationship between the dependency and contribution scores. Figure 4-6 provides a block definition diagram that shows the dependency-type constraint blocks owned by the safeguard subsystem.

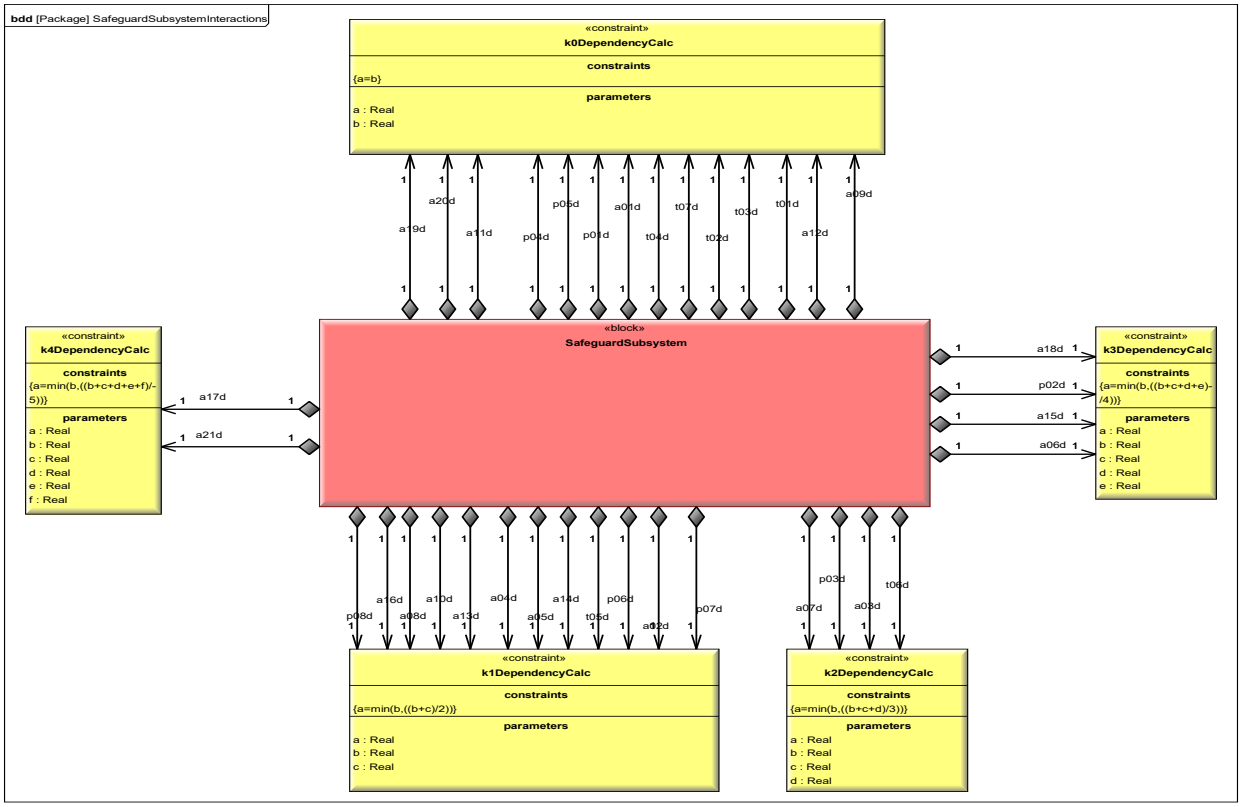


Figure 4-6 Safeguard subsystem interactions block definition diagram

4.3.1.3.3 Contributor Subsystem (Constraint-Type) Constraint Blocks

Constraint-type constraint blocks are used for defining the relationship shown in equation 3.3 for each corresponding safeguard. Similar to the contribution-type constraint blocks, unique constraint blocks were required for capturing contributor-contributor interactions due to the use of aggregate value properties for *ctr* and *cti*. As shown in Figure 4-7, 20 constraint blocks were defined resulting in 20 unique constraint properties for the contributor subsystem.

.

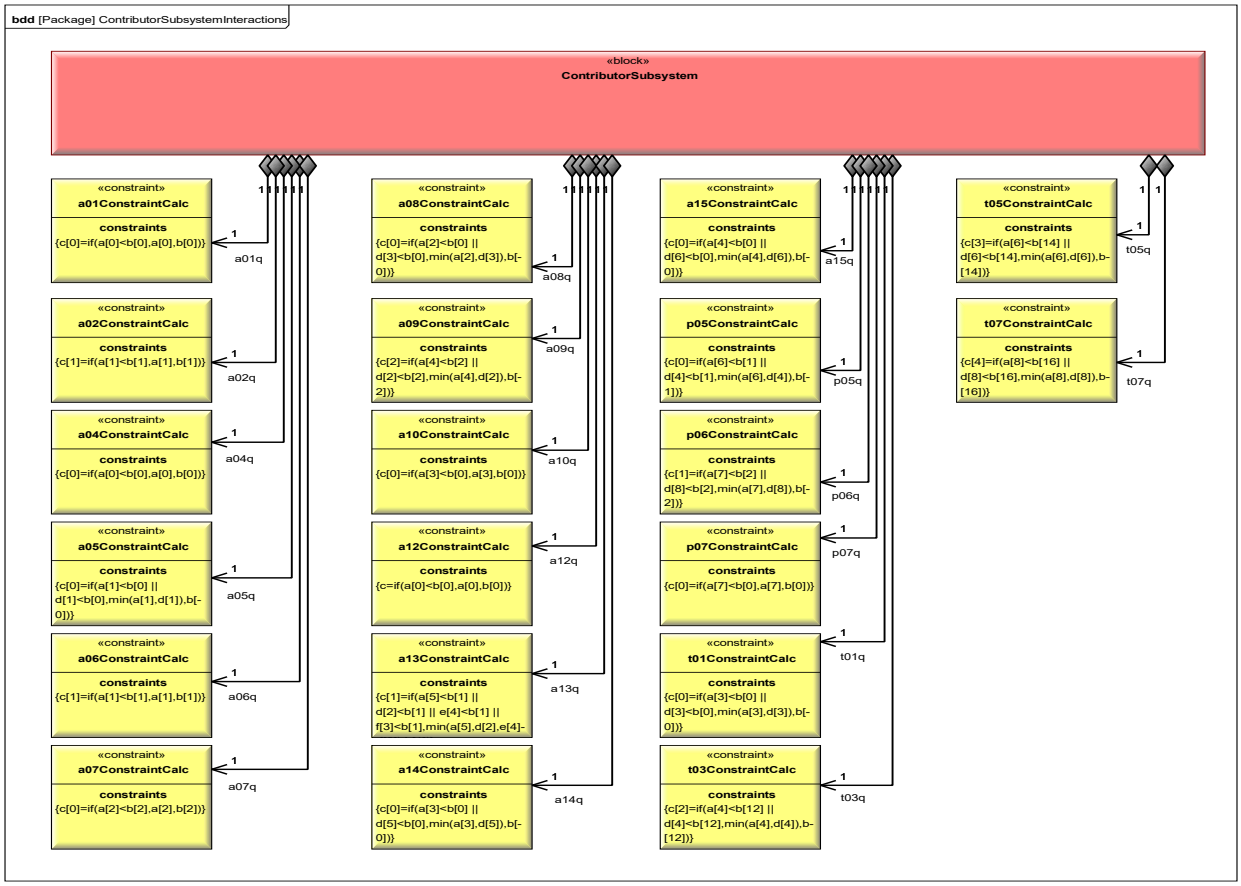


Figure 4-7 Contributor subsystem interactions block definition diagram

4.3.1.3.4 Confidentiality (p_1) Calculation Constraint Block

In order to define a calculation for p_1 within the ISS, a p_1Calc constraint block was defined for equation 3.4. This block is typed by the ISS, giving it a constraint property for the overall system-level measure of confidentiality. Because of the nature of equation 3.4, it is possible that attempts to solve this equation could result in a divide by zero error should all of the safeguard weights be set to 0 during instantiation. Because it is expected that the case of zero

weight safeguards would not produce a measure for p_1, an additional logical check was added to the p_1Calc constraint block to prevent this boundary-condition error during instantiation. Figure 4-8 illustrates the p_1Calc constraint block and the corresponding equation for overall ISS confidentiality.

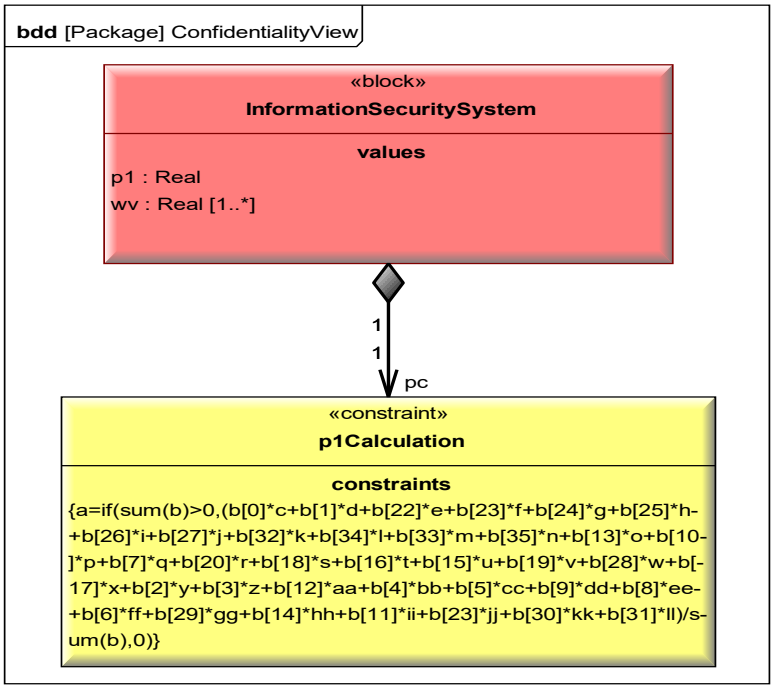


Figure 4-8 Confidentiality view block definition diagram

4.3.2 Parametric Diagrams

Parametric diagrams are used for further defining constraint properties through the binding of block value properties to equation parameters defined in the corresponding constraint blocks. This process provides a mechanism for relating value properties across an entire system

subject to a set of constraints, and therefore provides the ability to analyze quantitative systemic characteristics. With respect to the ISM, the collection of parametric diagrams details the network of calculations used for measuring confidentiality as an emergent information security system property.

Each block in the ISM with constraint properties, specifically as discussed in Section 4.3.1.3, has a corresponding set of parametric diagrams. The parametric diagrams for each block are described in the following subsections. Due to the size of the parametric diagrams, excerpts are provided in the relevant subsections below. The intent is to provide diagram portions for facilitating the discussion of each type of parametric diagram used in the ISM, while maintaining readability of the document. All ISM diagrams in their entirety are provided for reference in Appendix A.

4.3.2.1 Information Security System Parametric Diagrams

The information security system block owns 6 parametric diagrams for calculating the contribution scores of safeguards. The rationale for 6 individual diagrams was for manageability – SysML does not require that all of a block's constraint properties and associated bindings appear on a single parametric diagram. Figure 4-9 provides an excerpt of an ISS contribution parametric diagram which depicts the binding of values among two safeguards, two information security system contribution constraint properties, and the 5 associated contributor elements.

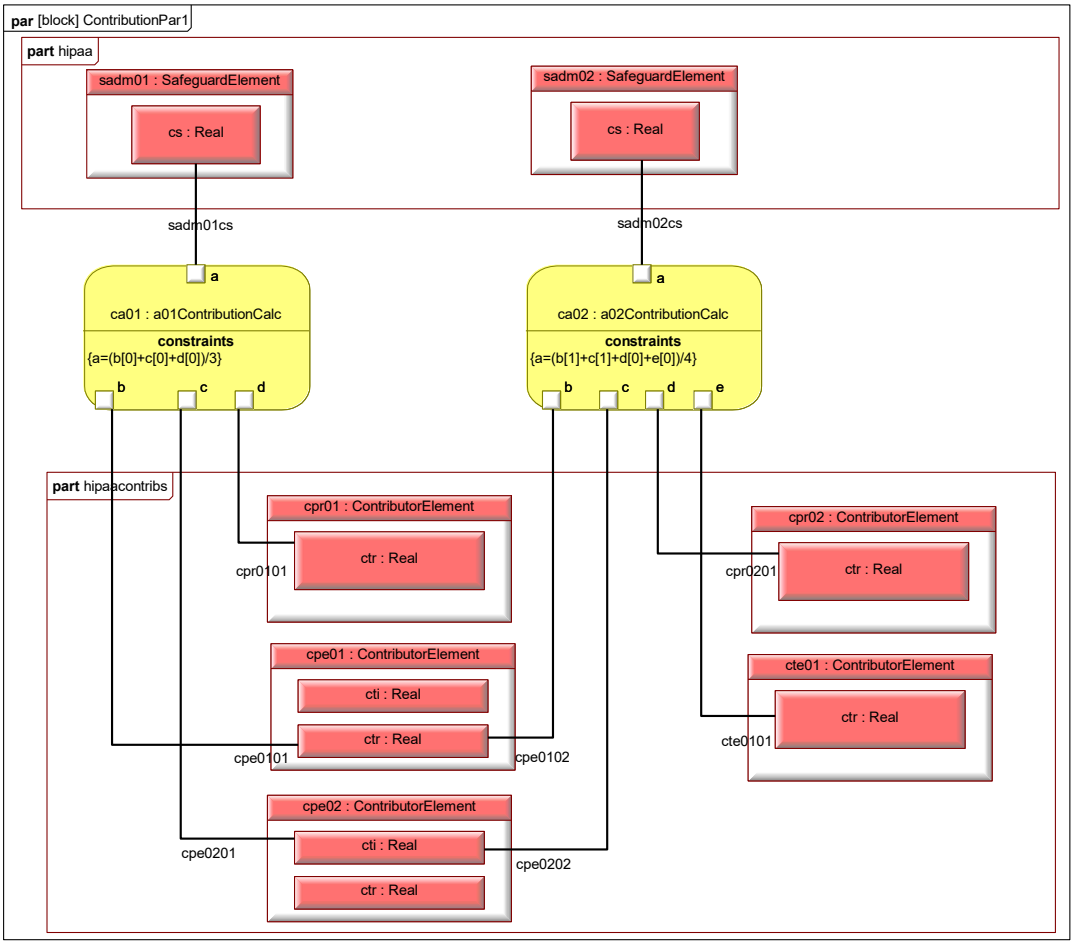


Figure 4-9 Excerpt of ISS level contribution parametric diagram

As shown in Figure 4-9, the hipaa and hipaacontribs part properties of the information security system are represented by *frames*, which contain the respective safeguard and contributor elements. Additionally, the value properties of these elements are exposed, and the binding to each equation parameter is visible.

The information security system owns one additional parametric diagram for calculating confidentiality. A portion of the confidentiality parametric diagram is shown in Figure 4-10.

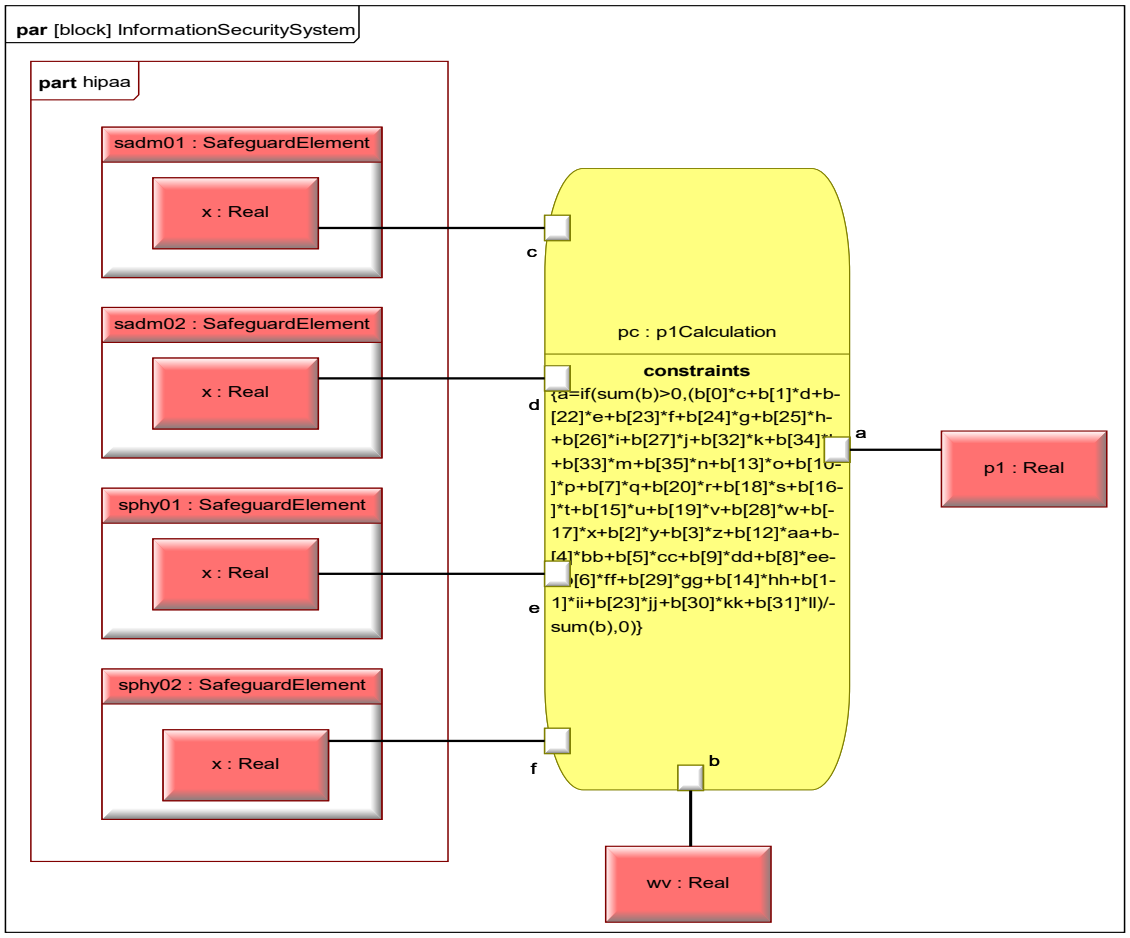


Figure 4-10 Portion of confidentiality parametric diagram

Note that the constraint equation indicates the terms for 36 safeguard elements, although only four safeguards are shown (for diagram readability). Additionally, the value properties for p_1 and *wv* do not appear in a frame as they are not defined by a part property, but belong to the owning block (i.e. the information security system) itself.

4.3.2.2 Safeguard Subsystem Parametrics Diagrams

The safeguard subsystem owns three parametric diagrams for calculating the dependency scores for each safeguard element. Like contribution parametric diagrams, multiple dependency parametric diagrams were used as opposed to a single and large diagram. Figure 4-11 provides a sample safeguard subsystem dependency parametric diagram.

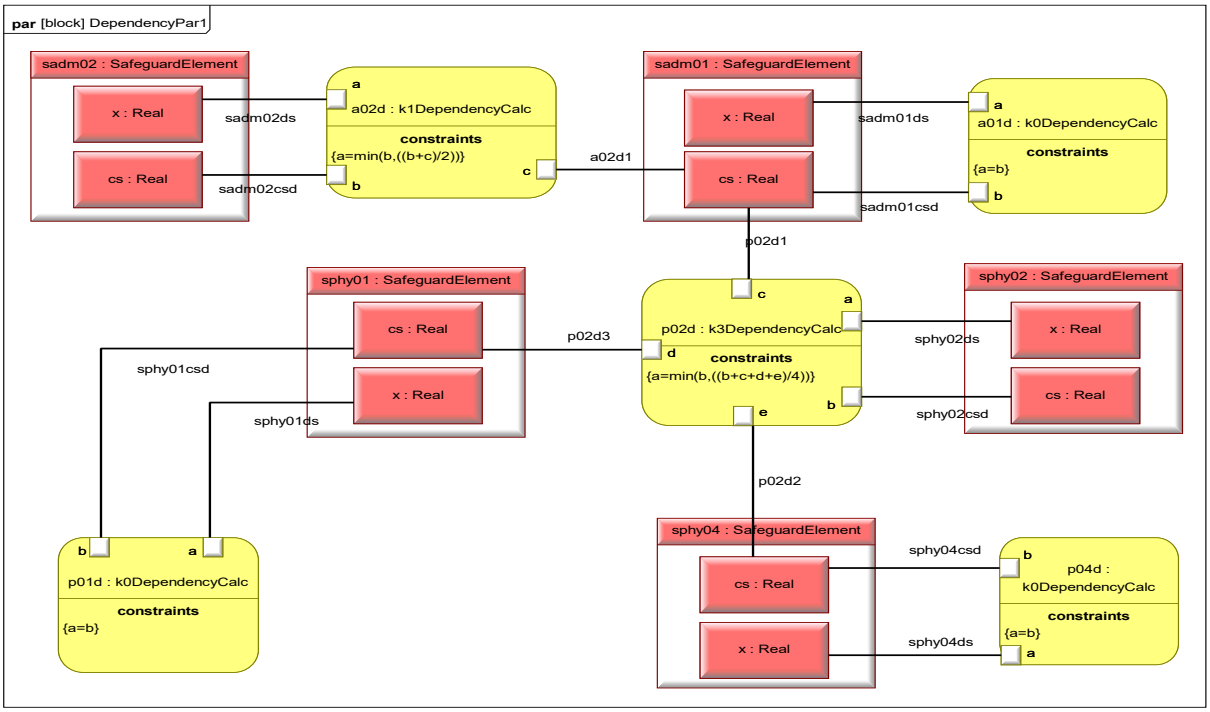


Figure 4-11 Excerpt of safeguard subsystem parametric diagram

The dependency parametric diagram shown in Figure 4-11 illustrates the calculation of safeguard dependency scores as defined in equation 3.2 using the *cs* values for dependent

safeguards. Figure 4-11 also shows the case of k0 constraints, in which the *cs* and *x* values for a safeguard are equivalent.

4.3.2.3 Contributor Subsystem Parametric Diagrams

The contributor subsystem contains one constraint parametric diagram which captures all of the corresponding constraint properties. Figure 4-12 provides an excerpt of the contributor subsystem parametric diagram which depicts the contributor-contributor interactions for safeguard sadm013 (identified in the constraint property as "a13q: a13ConstraintCalc"), in which the cpr04 contributor element is constrained by contributor elements cpe04, cpe05, cpe06, and cpe07.

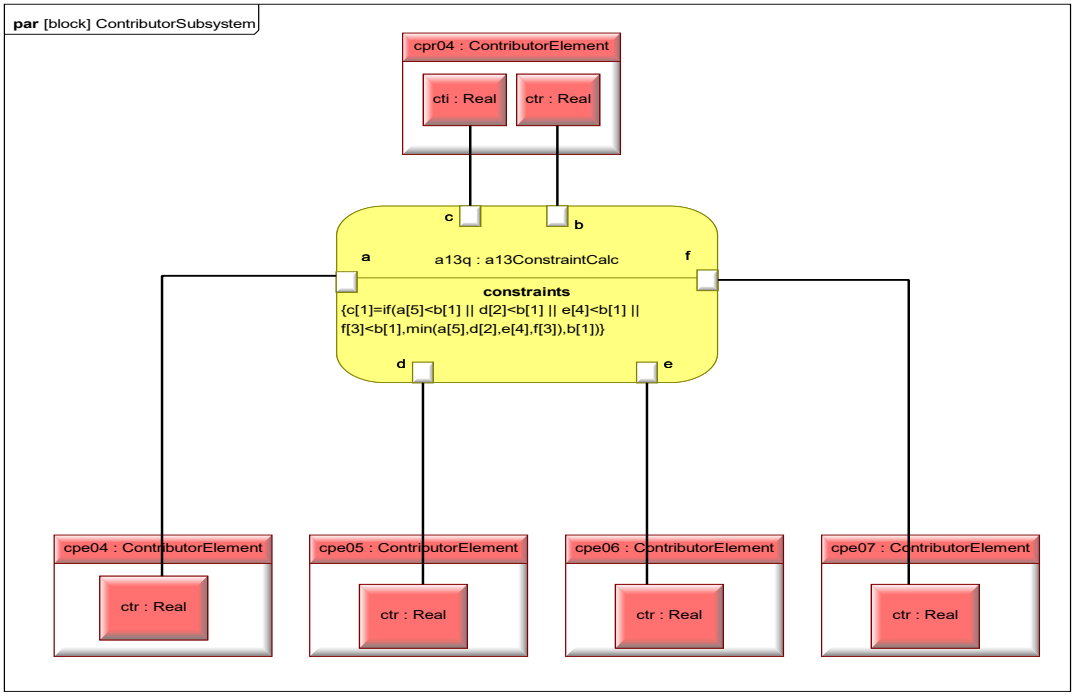


Figure 4-12 Excerpt of contributor subsystem constraint parametric diagram

The constraint property shown in Figure 4-12 illustrates that a more-complex logical statement was required for determining the cti value for a contributor according to equation 3.3. This results from the nature of the constraint which is based on a comparison of values as opposed to strictly a calculation.

4.4 ISM Instance Model

The instance model defines a specific instance of the ISM structure model using an object diagram. The object diagram contains *instances* of the blocks defined in the structure model and enforces all of the structural properties (value, part, and constraint) defined in the structure model. Each instance contains *slots* which correspond to its properties. Of specific interest are the slots which represent value properties, which will contain user-defined input variables, in addition to all values calculated via parametric solving. Table 4-3 identifies the structure model block and the corresponding number of instances specified in the instance model.

Table 4-3 Object diagram instances and quantity

Structure Model Block	Instance Count
Organization	1
Information Security System	1
Safeguard Subsystem	1
Contributor Subsystem	1
Safeguard Element	36
Contributor Element	46

The details of populating slot values and solving are deferred to Chapter 5 as the intent of this section is to introduce the ISM object diagram and relevant instance model concepts. The ISM contains a single object diagram which holds all instances. A portion of the ISM object diagram is shown in Figure 4-13.

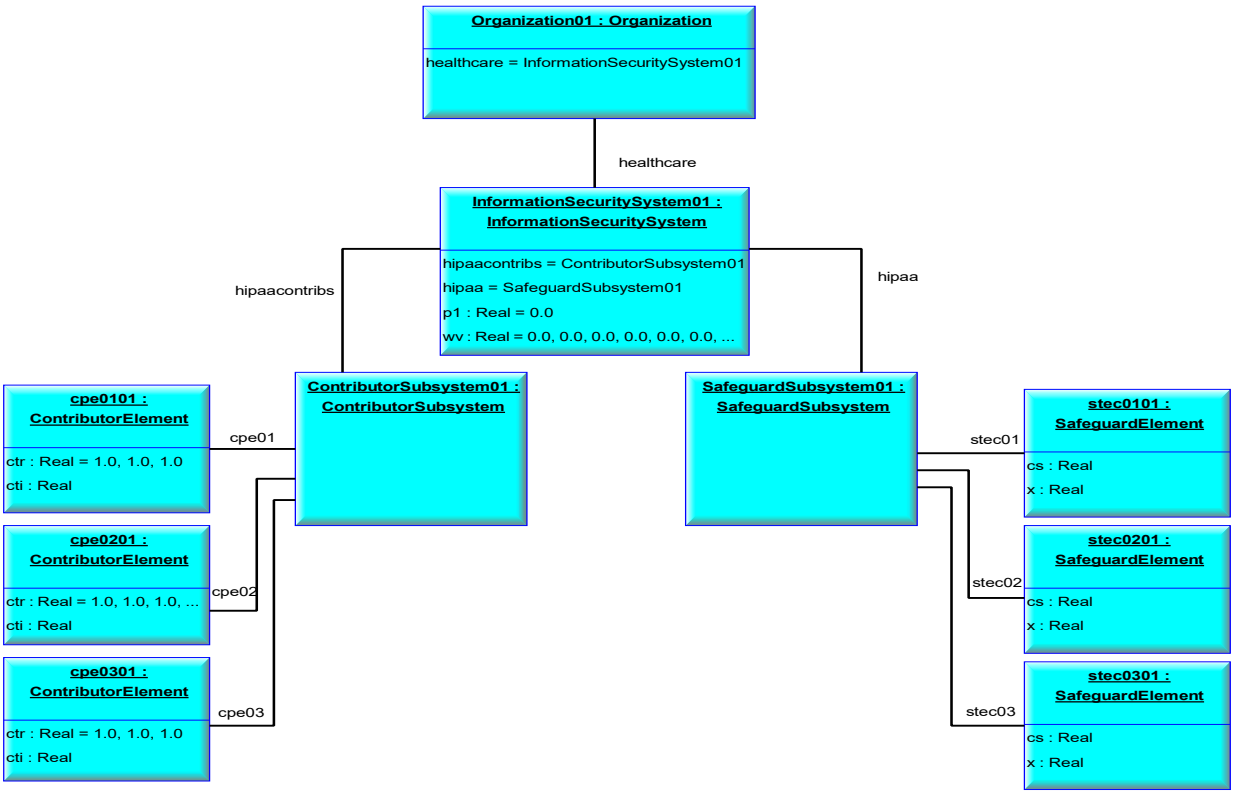


Figure 4-13 Excerpt of ISM instance model object diagram with slots shown

4.5 Summary

In this chapter, an ISM was developed for implementing the measurement approach developed in Chapter 3. A system model capable of being instantiated was constructed using SysML. In the next chapter the ISM instantiation process is described, and several experiments are performed to demonstrate the ability of the ISM to generate a measure of confidentiality.

CHAPTER 5

ISM INSTANTIATION AND RESULTS

5.1 Introduction

In this chapter, the ISM developed in Chapter 4 is instantiated for the purpose of generating a measure of confidentiality. This was accomplished by populating the ISM instance model with user input values and solving using ParaSolver. The primary objective was to demonstrate the ability of the ISM to be instantiated using a set of initial input values. Several verification tests were performed to confirm that the ISM accurately represented the conceptual measurement approach defined in Chapter 3. Additionally, a set of experiments was performed to assess changes in the measure of confidentiality by varying the minimum and maximum contribution input values for each type of contributor. The illustration shown in Figure 5-1 provides an overview of the ISM instantiation process.

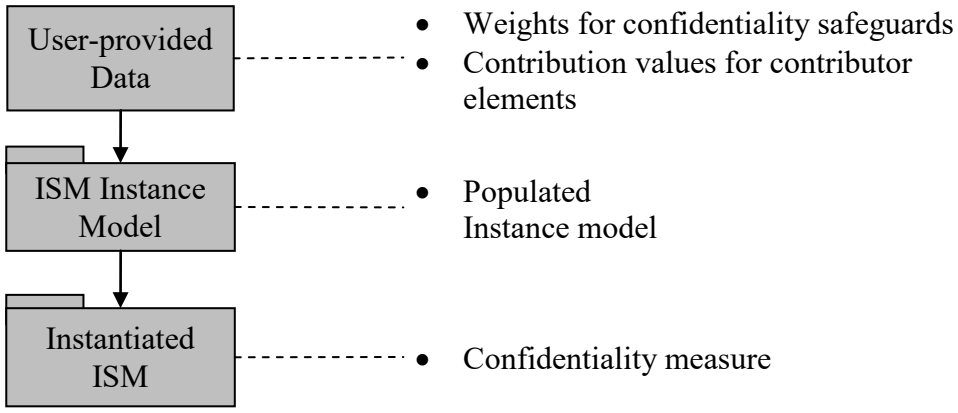


Figure 5-1 ISM instantiation overview

5.2 Description of Experiments

As previously stated, the primary objective of this chapter is to demonstrate the ability of the ISM to be instantiated therefore demonstrating the capability of the overall measurement approach to generate a measure of confidentiality. In this section, several tests and experiments consisting of one or more instantiations are described for meeting this objective.

5.2.1 Model Verification Tests

Three verification tests were performed to determine if the conceptual measurement steps developed in Section 3.5 were implemented correctly (i.e. as intended) in the ISM. These tests are described below.

5.2.1.1 1's Ctr Test

An instantiation using a value of 1.00 for the ctr slot value for each contributor instance was performed. The objective of this test is to verify the upper bound on p_1, specifically the maximum value of confidentiality that can exist in the ISS if all contributors are contributing their maximum value. A weight value of 1.00 for all safeguards was assumed. The value of p_1 returned by ParaSolver after solving the instance should be 1.00.

5.2.1.2 0's Ctr Test

An instantiation using a value of 0.00 for the ctr slot value for each contributor instance was performed. The objective of this test is to verify the lower bound on p_1, specifically the minimum value of confidentiality that can exist in the ISS if all contributors are contributing

their minimum value. A weight value of 1.00 for all safeguards was assumed. The value of p_1 returned by ParaSolver after solving the instance should be 0.00.

5.2.1.3 ParaSolver Browser Test

Although not based on specific instance model input values, the ParaSolver browser itself performs a validation of the SysML structure model prior to loading. This is similar to a compile-time check and indicates the existence of diagramming errors (e.g. missing connectors). Additionally, the browser check will identify certain instance model errors, such as uninitialized parameters or unpopulated slots for which values are required. Because in all cases the ParaSolver browser must load prior to solving, each instantiation can be viewed as being structurally validated with respect to ParaSolver.

5.2.2 Boundary Experiments

Six additional experiments (instantiations) were performed to assess the change in the value of p_1 predicated by varying the contribution input values for each *type* of contributor. This experiment consisted of 6 individual instantiations in which the ctr values for combinations of contributor types were set to their minimum (ctr = 0.00) and maximum (ctr = 1.00). A weight value of 1.00 for all safeguards was assumed, indicating an equal importance of each HIPAA Security Rule safeguard in the calculation of p_1. Table 5-1 illustrates the combinations of *ctr* values and contributor types utilized in the experiments.

Table 5-1 Boundary experiment table

Contributor Type	Experiment 1 ctr value	2 ctr value	3 ctr value	4 ctr value	5 ctr value	6 ctr value
People	1.00	1.00	1.00	0.00	0.00	0.00
Process	1.00	0.00	0.00	1.00	0.00	1.00
Technology	0.00	0.00	1.00	0.00	1.00	1.00

5.3 Model Inputs and ParaSolver Setup

5.3.1 Instance Model Inputs

ParaSolver provides an interface with Microsoft Excel, which can be used to import spreadsheets containing input values into the ISM instance model within Artisan Studio. Setting up the interface involved linking the *ctr* and *wv* slot values in the instance model to the corresponding rows/columns in the spreadsheet containing input values. The initial setup is only performed once and subsequent instantiations can be performed by modifying the input values in the spreadsheet, and re-importing into the instance model. The Excel interface was particularly advantageous for managing the values associated with the *ctr* and *wv* aggregate value properties.

An ISM Data.xlsx spreadsheet was created for holding instance model input and output values (model output is further discussed in Section 5.4). Instance model inputs are contained in the “ctr input matrix” tab. Additionally the spreadsheet contains a “ctr verification matrix” tab, which documents the mapping of each contributor slot to the corresponding safeguard. Figure

5-2 provides a screen capture of the ISM Data.xls spreadsheet, with the ctr input matrix tab shown.

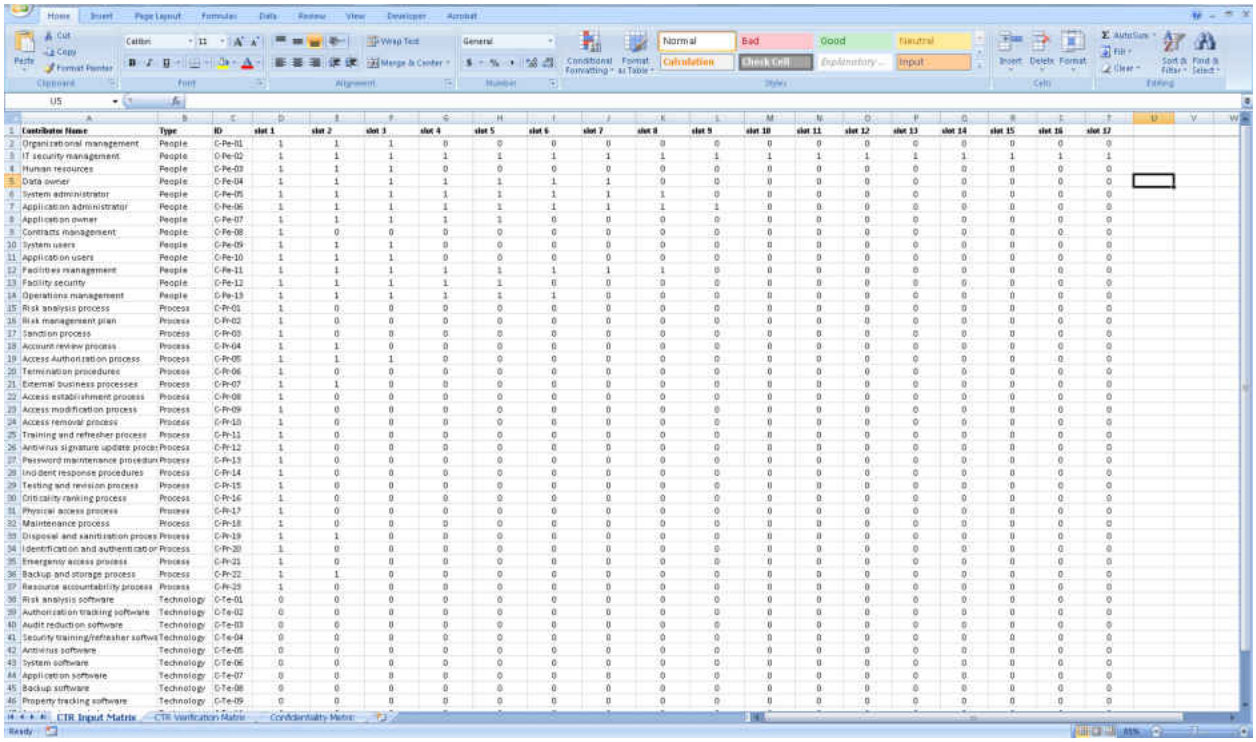


Figure 5-2 ISM Data.xlsx spreadsheet

5.3.2 Browser Initialization

Once the Excel interface has been executed for a set of input values, the structure and instance model headings are created, and the ParaSolver browser is launched. Headings are used to define the *root* block in the structure model, in this case the Organization block, and to version the instance model be solved. These headings are referred to as CXS and CXI, respectively.

When the ParaSolver browser is launched, the structure and instance model data is parsed into the appropriate data structures for solving using the external Mathematica solver. As mentioned earlier, when the browser is successfully launched, the indication is that the integrity of the structure model has been successfully validated. Figure 5-3 shows the ParaSolver browser following a successful launch within the Artisan Studio modeling environment.

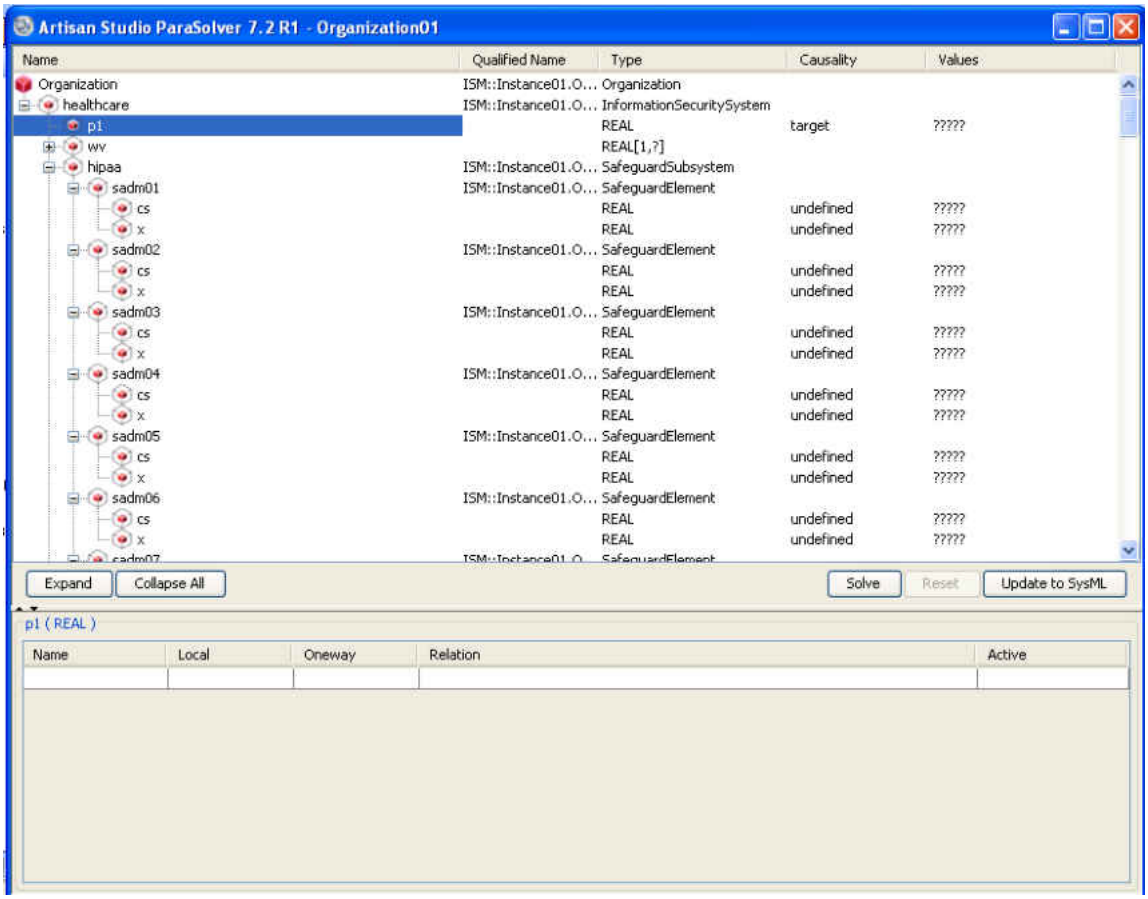


Figure 5-3 ParaSolver browser following successful launch

5.3.3 Variables and Causality

Prior to solving, a *causality* state must be assigned to each variable (i.e. value property) used in solving for p_1. Causality refers to the relationship among variables within parametric equations. ParaSolver requires that one of four causality states be assigned to each variable prior to solving. These states are:

1) Given: known value provided by the user before solving.
2) Target: unknown value of which the user desires to calculate.
3) Undefined: unknown value which may be calculated in solving for the target.
4) Ancillary: unknown value prior to solving - calculated during solving and used to calculate the value of another variable.

Once the ParaSolver browser loads, all variables are initially set to the undefined causality state. It is only necessary to change the causality of p_1 to target. All *ctr* and *wv* values are automatically set to a given state based on being imported via the Excel interface. All remaining variables remain undefined. Table 5-2 provides a summary of each variable and identifies the initial and final causality states for each.

Table 5-2 Variable definition, multiplicity, and causality assignment

Variable	Multiplicity	Description	Initial Causality	Final Causality
p_1	1	Value property owned by the ISS block. Calculated using parametric equations (i.e. interactions) defined with the ISS, safeguard, and contributor subsystems. Represents the measure of confidentiality.	Target	Target
wv	1…*	Aggregate value property owned by the ISS block. Contains 36 real values and represents a vector of safeguard weights.	Given	Given
ctr	1…*	Aggregate value property owned by a contributor block. Contains one or more contribution values for each safeguard to which it contributes.	Given	Given
cti	1…*	Aggregate value property owned by a contributor block. Contains modified ctr values for each safeguard (i.e. ctr value affected by a contributor-contributor interaction within the contributor subsystem).	Undefined	Ancillary
cs	1	Value property owned by a safeguard block. Represents the contribution score and is used in the calculation of x.	Undefined	Ancillary
x	1	Value property owned by a safeguard block. Represents the safeguard dependency score.	Undefined	Ancillary

5.4 Output and Analysis

ParaSolver reports solution results in the application browser within the Artisan Studio modeling environment as shown in Figure 5-4. Additionally it provides an interface for writing values to Excel. For each instantiation, all x values and p_1 results were written back to a tab in

the ctr matrix spreadsheet to populate the confidentiality metric (confidentiality metric tab). The results of all instantiations discussed in this section are included in Appendix B.

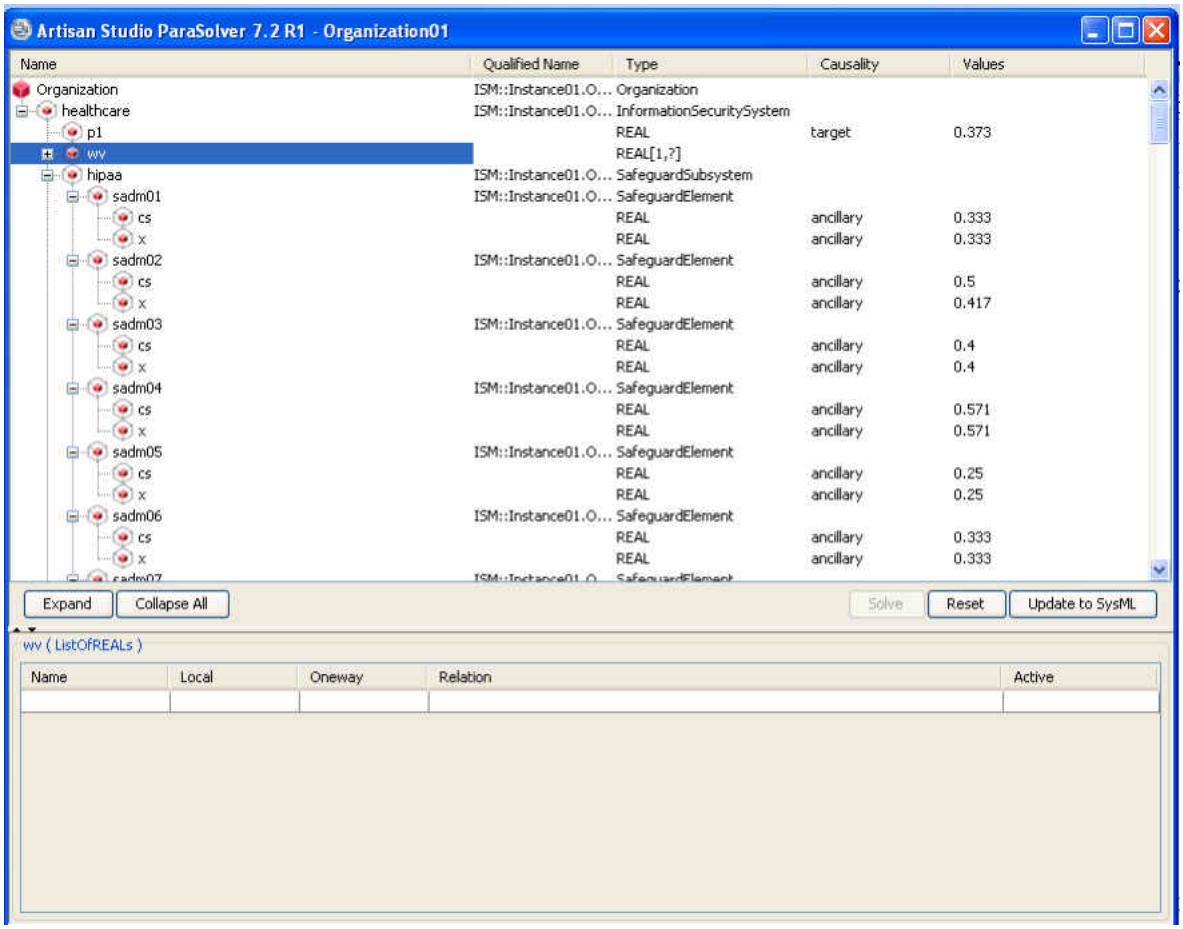


Figure 5-4 ParaSolver browser following solving

5.4.1 Model Verification Results

5.4.1.1 1's Ctr Test

The resulting solution provided by ParaSolver was a p_1 value of 1.00 as expected.

5.4.1.2 0's Ctr Test

The resulting solution provided by ParaSolver was a p_1 value of 0.00 as expected.

5.4.2 Additional Experiments

The additional boundary experiments identified in 5.2.2 provide an indication of how people, process, and technology contributors affect the overall measure of confidentiality in the ISS. The results of these experiments are illustrated in Figure 5-5

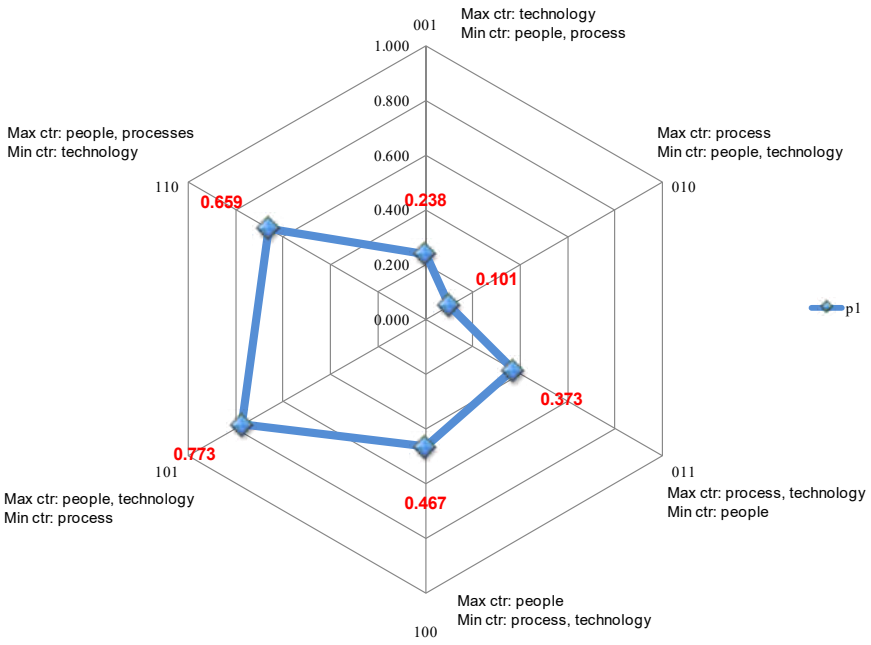


Figure 5-5 Plot of p_1 results for boundary experiments

As shown in Figure 5-5, p_1 most dramatically changes when the *ctr* values for people and technology contributors are at their minimum, the process *ctr* values are at their maximum and

then these conditions are reversed resulting in an increase in p_1 from 0.101 to 0.773. The indication is that people and technology contributors participate together in a high number of contribution-type interactions. Additionally, the lowest p_1 value (0.101) results when *only* process contributors are contributing to safeguards. The interpretation here is that that processes alone are not sufficient for maintaining confidentiality, a concept which was first introduced in Chapter 2.

Also of significant interest is that the three lowest p_1 values (0.238, 0.101, 0.373) all occur when the *ctr* values for *all people contributors* are 0. From the perspective of the ISM, this indicates that there are a high number of people-type contributors that participate in contribution-type interactions. As the corresponding *ctr* values go to 0, the *cs* and *x* scores calculated using these values begin to drop across the safeguard subsystem. In practice, this underscores the point introduced in Chapter 2 that organizational information security is not just a technical matter, but indeed people play a significant role in the protection of electronic information.

5.4.3 Confidentiality Metric

Using the Excel interface, the confidentiality metric tab of the ISM Data.xlsx spreadsheet was populated following each model instantiation. Figure 5-6 provides an example confidentiality metric generated using the ParaSolver output. The content of the confidentiality metric is consistent with that described in Section 3.6.

Safeguard	Type	ID	Dependency Score (x)	Confidentiality Weight (w)	wx	p1 value
Risk Analysis	Administrative	S-Adm-01	0.333	1.00	0.333	0.373
Risk Management	Administrative	S-Adm-02	0.417	1.00	0.417	
Sanction Policy	Administrative	S-Adm-03	0.400	1.00	0.400	
Information System Activity Review	Administrative	S-Adm-04	0.571	1.00	0.571	
Authorization and/or Supervision	Administrative	S-Adm-05	0.250	1.00	0.250	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.333	1.00	0.333	
Termination Procedures	Administrative	S-Adm-07	0.333	1.00	0.333	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	0.000	1.00	0.000	
Access Authorization	Administrative	S-Adm-09	0.250	1.00	0.250	
Access Establishment and Modification	Administrative	S-Adm-10	0.375	1.00	0.375	
Security Reminders	Administrative	S-Adm-11	0.400	1.00	0.400	
Protection from Malicious Software	Administrative	S-Adm-12	0.500	1.00	0.500	
Log-in Monitoring	Administrative	S-Adm-13	0.375	1.00	0.375	
Password Management	Administrative	S-Adm-14	0.400	1.00	0.400	
Response and Reporting	Administrative	S-Adm-15	0.000	1.00	0.000	
Data Backup Plan	Administrative	S-Adm-16	0.500	1.00	0.500	
Disaster Recovery Plan	Administrative	S-Adm-17	0.000	1.00	0.000	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.000	1.00	0.000	
Testing and Revision Procedure	Administrative	S-Adm-19	0.167	1.00	0.167	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	0.333	1.00	0.333	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.233	1.00	0.233	
Contingency Operations	Physical	S-Phy-01	0.000	1.00	0.000	
Facility Security Plan	Physical	S-Phy-02	0.000	1.00	0.000	
Access Control and Validation Procedures	Physical	S-Phy-03	0.472	1.00	0.472	
Maintenance Records	Physical	S-Phy-04	0.500	1.00	0.500	
Disposal	Physical	S-Phy-05	0.400	1.00	0.400	
Media Re-use	Physical	S-Phy-06	0.400	1.00	0.400	
Accountability	Physical	S-Phy-07	0.250	1.00	0.250	
Data Backup and Storage	Physical	S-Phy-08	0.667	1.00	0.667	
Unique User Identification	Technical	S-Tec-01	0.750	1.00	0.750	
Emergency Access Procedure	Technical	S-Tec-02	0.500	1.00	0.500	
Automatic Logoff	Technical	S-Tec-03	0.667	1.00	0.667	
Encryption and Decryption	Technical	S-Tec-04	0.667	1.00	0.667	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	0.667	1.00	0.667	
Integrity Controls	Technical	S-Tec-06	0.667	1.00	0.667	
Encryption	Technical	S-Tec-07	0.667	1.00	0.667	

Figure 5-6 Confidentiality metric generated using ParaSolver

5.5 Summary

In this chapter, the ISM's ability to generate a measure of confidentiality was demonstrated. Additionally, this served the dual purpose of demonstrating the measurement approach developed in Chapter 3. The results obtained verify the proper implementation of the

measurement approach and conceptual ISS and demonstrate the ability of the ISM to generate a quantitative measure of confidentiality using a set of user-provided input values.

CHAPTER 6

CONCLUSION

6.1 Summary of Work

In this study, a new approach for measuring the confidentiality of electronic information in health-care related organizations was formulated. Through an analysis of the existing classes and types of general information security measurement approaches, it was determined that a number of underlying issues are present which prevent their direct adaptation to the problem of measuring the confidentiality of electronic information in complex organizational systems. In order to overcome some of these issues, a systemic perspective on information security and confidentiality was adopted. By identifying and investigating the systemic characteristics that are present among the HIPAA Security Rule safeguards and their respective people, process, and technology organizational contributors, an information security system (ISS) for assuring the confidentiality of electronic information in healthcare organizations was synthesized. Confidentiality – a desired emergent property of the ISS – was defined in terms of the systemic interactions present in the ISS. By quantifying these interactions, a measure for the protection of electronic information from unauthorized disclosure was developed.

The measurement approach was implemented and demonstrated using an ISM developed in SysML. The ISM specifies an ISS and the systemic interactions among the safeguard and contributor elements that are present using block definition diagrams. Using SysML parametric diagrams, the quantitative interactions among the 36 HIPAA Security Rule safeguards and 46 organizational contributors were modeled. Using ParaSolver's SysML parametric diagram

execution capability, multiple instantiations of the ISM were performed and measures of confidentiality were generated using user-defined input values for contribution values and safeguard confidentiality weights. The results verify the proper implementation of the measurement approach and conceptual ISS and demonstrate the ability of the ISM to generate a quantitative measure of confidentiality using a set of user-provided input values.

6.2 Significance of Work

The propagation of personal medical information throughout healthcare-related organizations facilitated by expansions in health information technology and digital patient records has increased the difficulty associated with determining how "well" the confidentiality of electronic information is being maintained. While information security standards define the requirements for securing the overall information technology and processing environment of an organization, there is a lack of standard methods for measuring the protection levels of electronic information using these standards. The research presented in this work provides a systems-based solution that addresses the challenges associated with measuring the protection of electronic information within organizations that deliver healthcare services.

The measurement philosophy adopted in this research is differentiated from the existing methods discussed in Chapter 2 in that it acknowledges the existence of a conceptual protection system that subsists within complex organizational environments. The core approach of synthesizing information security-relevant systems is advantageous in that information security

is addressed in a systemic context as opposed to the more-common approach of evaluating it with respect to individual protection mechanisms or hard systems in isolation.

The approach developed in this research offers organizations a new method for obtaining visibility regarding the status of their information security efforts. Such insight facilitates the ability to not only evaluate and improve their information security programs and demonstrate compliance with requisite information security standards, but more importantly it supports the execution of due-diligence and due-care in addressing stakeholder-specific concerns regarding the confidentiality of personal health information. The proposed approach is also significant in that provides the ability to perform "what-if" scenarios and assessments of change in confidentiality that result from new safeguard standards or changes in the contribution values of people, processes, or technology to safeguards.

Additionally, this work puts forth a generalized approach for addressing information security measurement that is independent of a specific implementation. The general approach is illustrated in Figure 6-1.

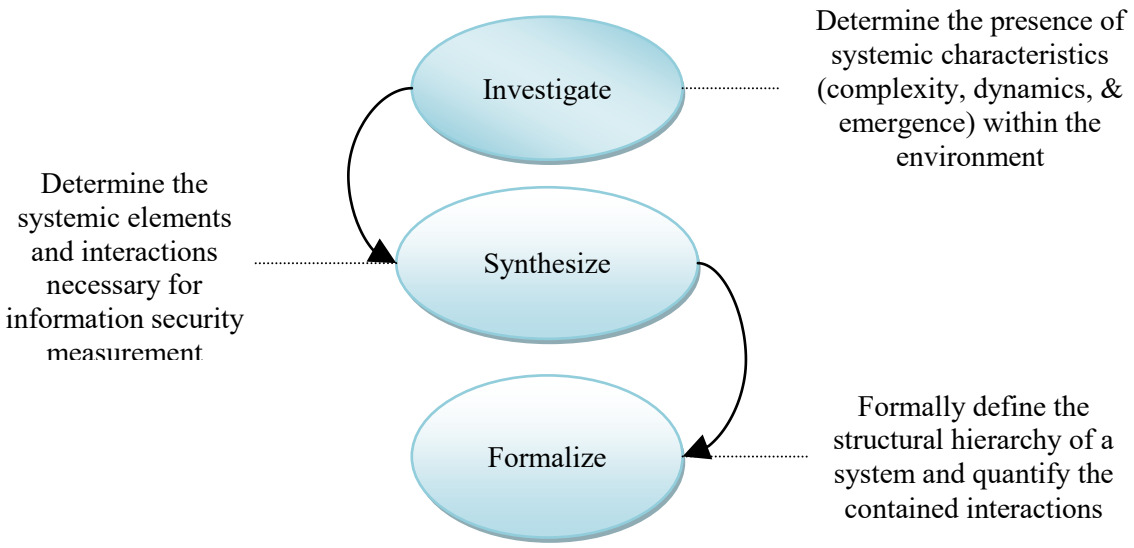


Figure 6-1 Measurement approach concept

6.2.1 Limitations and Assumptions

This measurement approach developed in this research assumes that the contribution values for each contributor and the confidentiality safeguard weights *can* be determined. That is, an approach for estimating these values is assumed, and is not developed in this study.

The lack of a unified approach for the large-scale validation of information security metrics is a problem endemic to information security research. Practical and legal challenges, in addition to organizations' reluctance to reveal the details of their information security control environments are some of the many roadblocks to large-scale validation of information security metrics and measurement approaches (Greer, Hoo, and Jaquith, 2010). The lack of historical data makes it difficult to perform macro or micro-level validation of results. This is in contrast to

other system-level properties, such as reliability, which have the benefit of more well-established models and analysis techniques.

However, the lack of universally-accepted validation methods should not preclude the development of new approaches for measuring the protection levels of electronic information. As noted by NIST (2010), most formal approaches for security measurement and assessment have achieved only limited success. This study focused on the development of a new approach and measurement paradigm for confidentiality and information security in an organizational context.

This study is germane to the general control environment within an organization, and does not attempt to address each of the individual security settings and parameters that exist within the hardware and software components present within an organization. In Chapter 3, it was discussed that a measure of confidentiality in the context of the overarching general control environment is a more-appropriate indicator as it addresses the function of a protection system. The intent of this research was to provide a good, yet *practical* measure of information security with respect to the general control environment.

6.3 Research Contributions

A primary contribution of this research is to the general body of knowledge regarding information security measurement, specifically within the healthcare domain. As evidenced by the literature review presented in Chapter 2, there is an observable lack of research regarding information security measurement and metrics specifically within the healthcare industry. This work provides an approach for measuring information security as it relates to the information

security requirements and standards of healthcare-related organizations. Table 6-1 provides a summary of the key contribution areas for this study.

Table 6-1 Summary of research contributions

Area of Contribution	Summary
Healthcare Information Security Measurement	This work provides an approach for measuring information security as it relates to the HIPAA Security Rule.
General Information Security Measurement	This research offers a new approach and measurement paradigm for confidentiality and information security measurement in general. The systemic solution proposed in this study provides a new way forward for measuring information security properties in terms of systemic elements which are present in a general control environment.
Enterprise-level Security Metrics	This study proposes a new metric for confidentiality that offers more fidelity than existing metrics by addressing the contributions from people, process, and technologies to safeguards in a systems context.

6.4 Future Research Directions

This study focused on the development of a new approach and measurement paradigm for information security. While the underlying theory for systemic information security measurement was presented and demonstrated, there are several key areas of future work to be explored. These areas are identified in the following subsections.

6.4.1 Extensibility

Although this study focused on the concept of a protection system (i.e. an ISS), the core concept of synthesizing information security-relevant systems can be extended to address other systems of interest. For example, threats and vulnerabilities are important information security concepts that will need to be addressed in future research efforts because of their effect on organizational efforts to protect electronic information.

Using the same approach discussed in Chapter 3, "threat" and "vulnerability" systems could be synthesized. Subsequently, their subsystems, elements, and interactions could be formalized and added to the ISM concept. The interaction between the ISS and the threat/vulnerability systems and elements could be investigated and the effect on confidentiality could be assessed. Such analysis would not only be beneficial for building a complete information security measurement approach, but would also be beneficial when new stakeholder concerns arise regarding a specific type of threat or vulnerability. Figure 6-2 provides an example of a hypothetical threat system in relation to an ISS as part of synthesis.

.

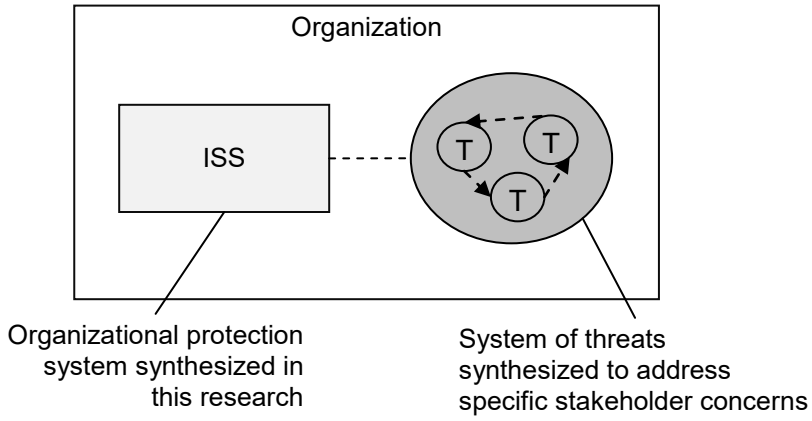


Figure 6-2 Organization, ISS, and hypothetical threat system

6.4.2 Additional Studies

Because this study is relative to development of a new measurement approach, the experiments discussed in Chapter 5 are relative to boundary conditions (i.e. min/max values for contributor types). A primary area for additional studies would be the development of methodology for determining (estimating) the contribution values for the various contributor elements and performing additional experiments using these values.

As stated in Section 6.2.1, validation is a key area of need affecting information security measurement and metrics in general. Additional studies should be performed to further validate the systemic approach for measuring confidentiality developed in this study. Application to information security standards and domains other than healthcare would also be beneficial for further validation of the measurement approach.

The integration of human behavior (e.g. social technical) models for estimating contribution values could add a powerful predictive and forecasting capability to the approach developed in this study. This distinction is important, as the solution proposed in this research involves capturing what a system "is doing", as opposed to what it "can do" over time. The former is measurement-focused where the latter is improvement-focused.

6.4.3 Metrics Aggregation

Another direction for future research relates to applying the proposed measurement approach to the remaining protection perspectives identified in the HIPAA Security Rule (i.e. integrity and availability). Such work would provide a foundation for secondary studies regarding the aggregation of information security metrics. The formal aggregation and composition of security properties and associated metrics is a significant challenge facing the information security research community. A consistent approach for measuring individual security properties is a critical element related to these efforts. Figure 6-3 illustrates the scope of this research in the context of future work related to information security metrics aggregation.

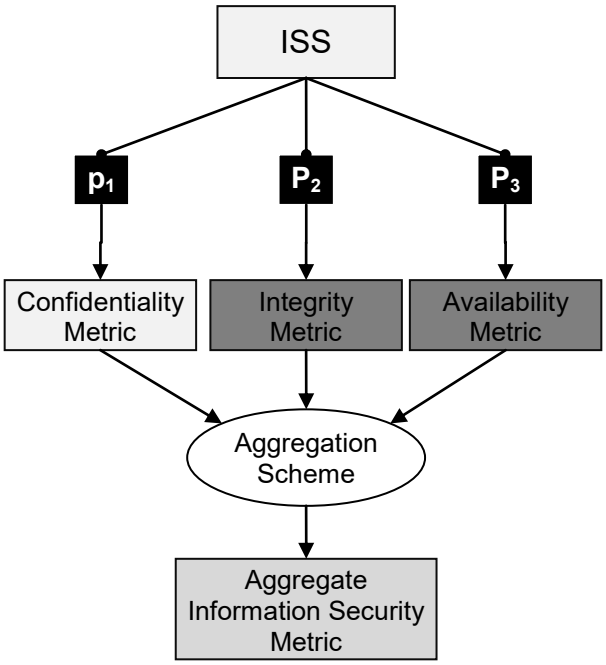
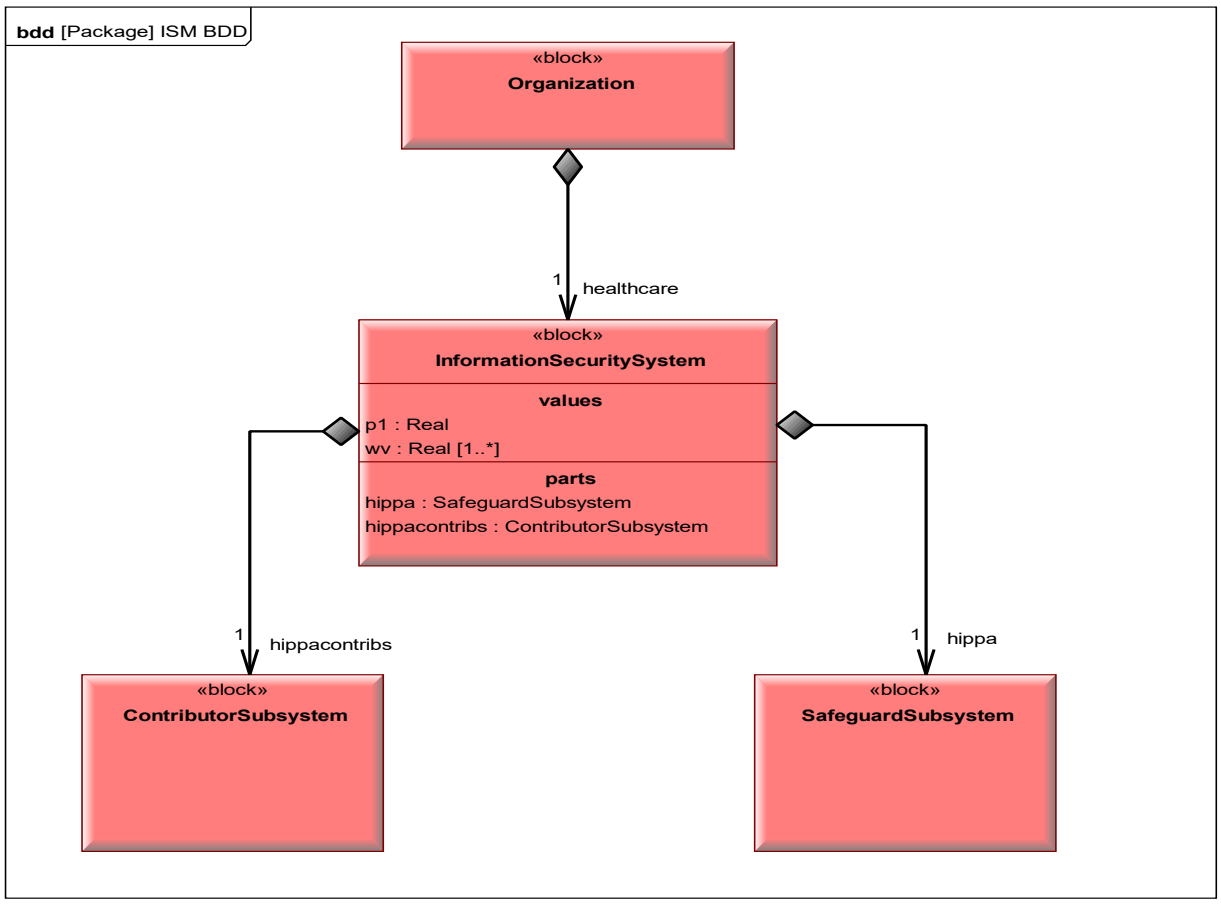
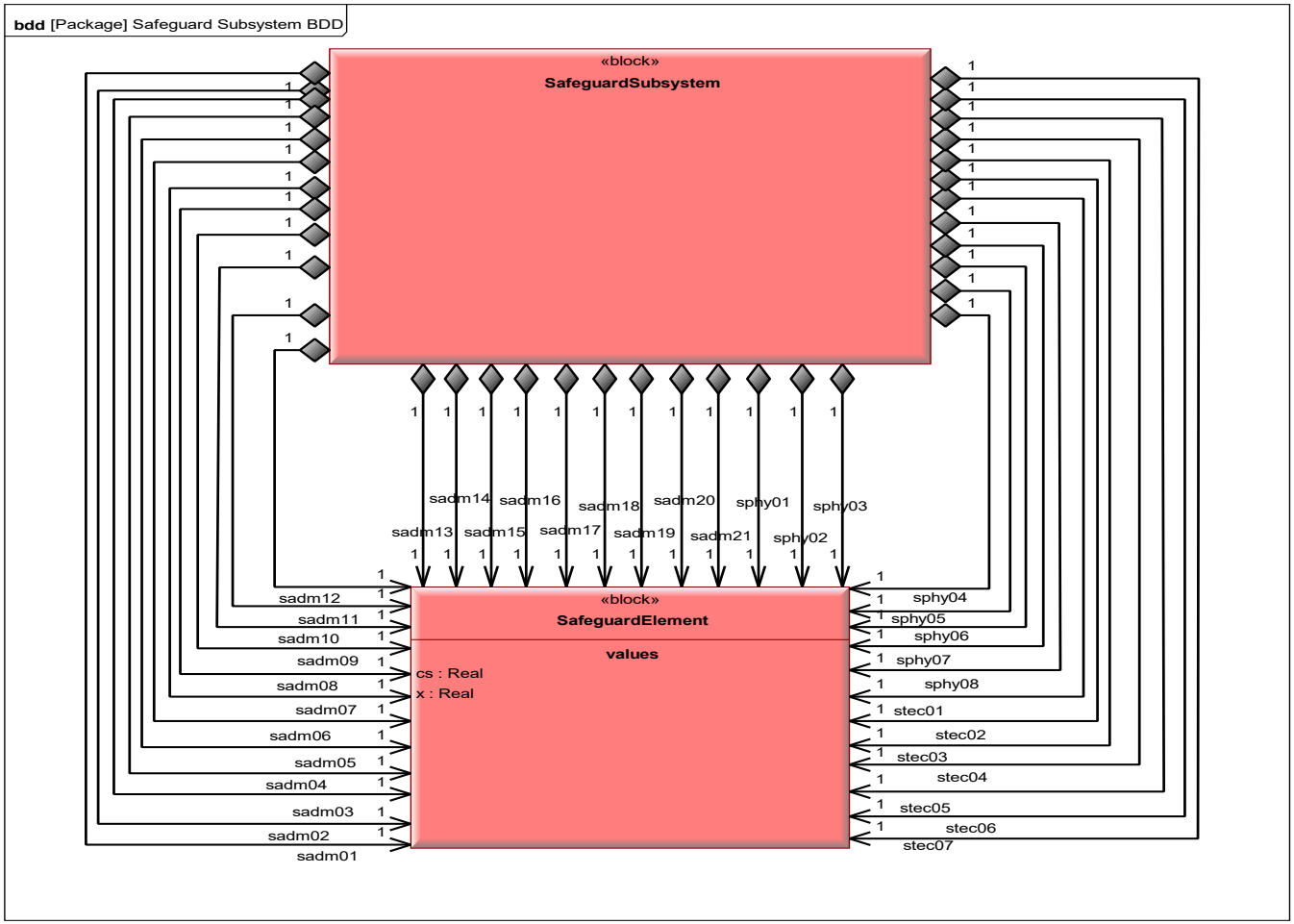


Figure 6-3 Information security metric aggregation

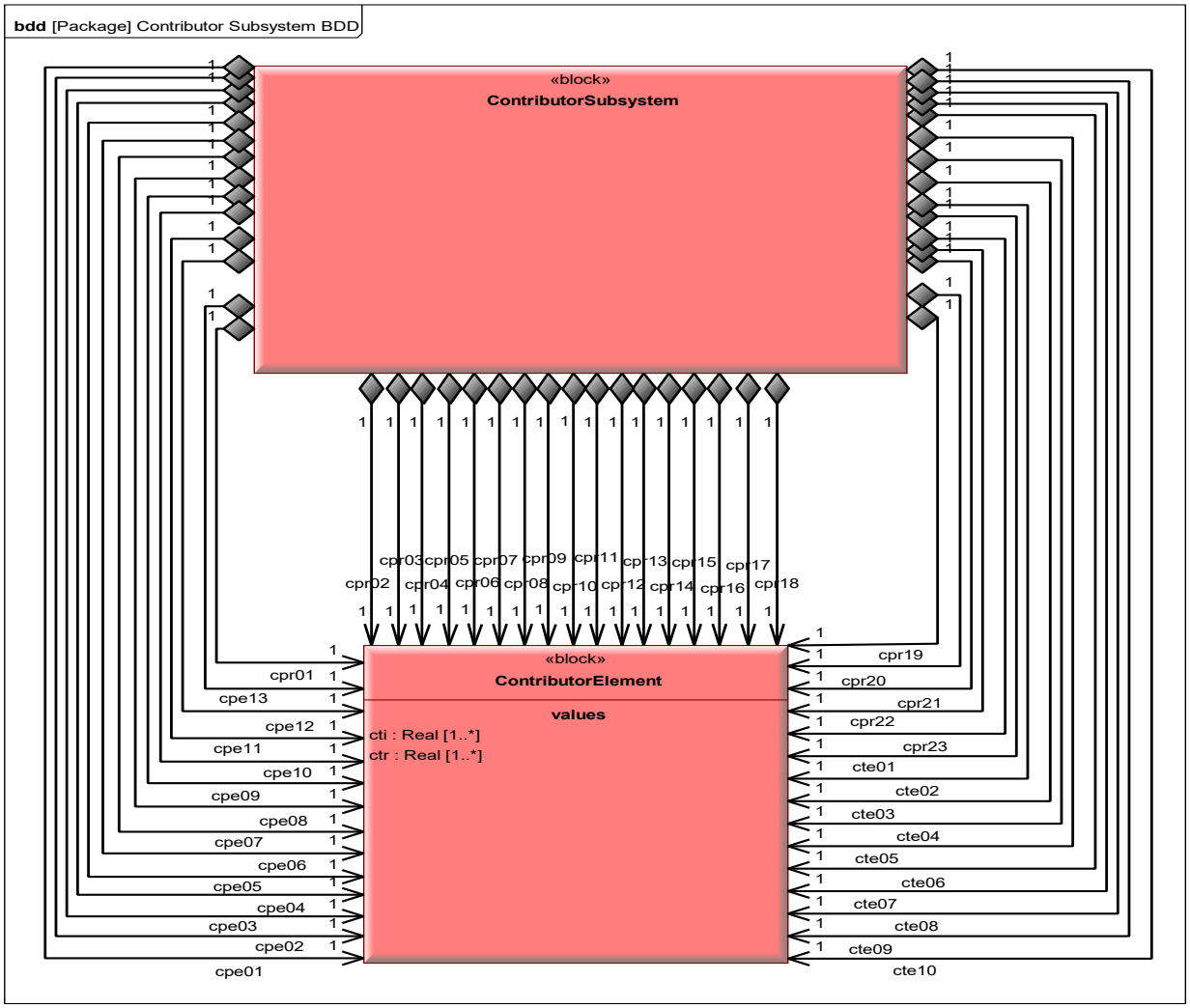
APPENDIX A: ISM DIAGRAM REFERENCE



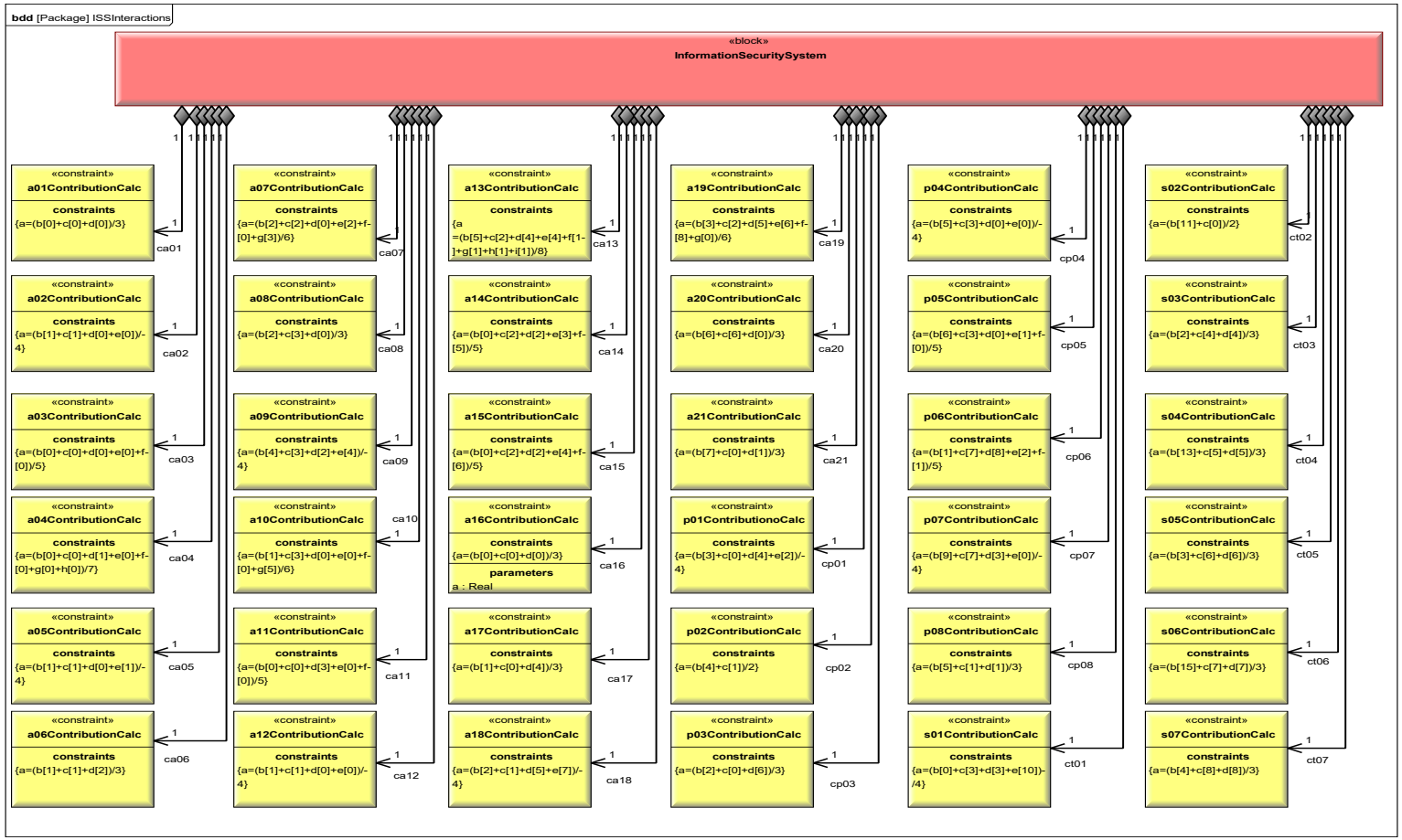
Name: [Package] ISM BDD
FullScopedName: ISM.[Package] ISM BDD
DynamicUmlClassName: BlockDefinitionDiagram



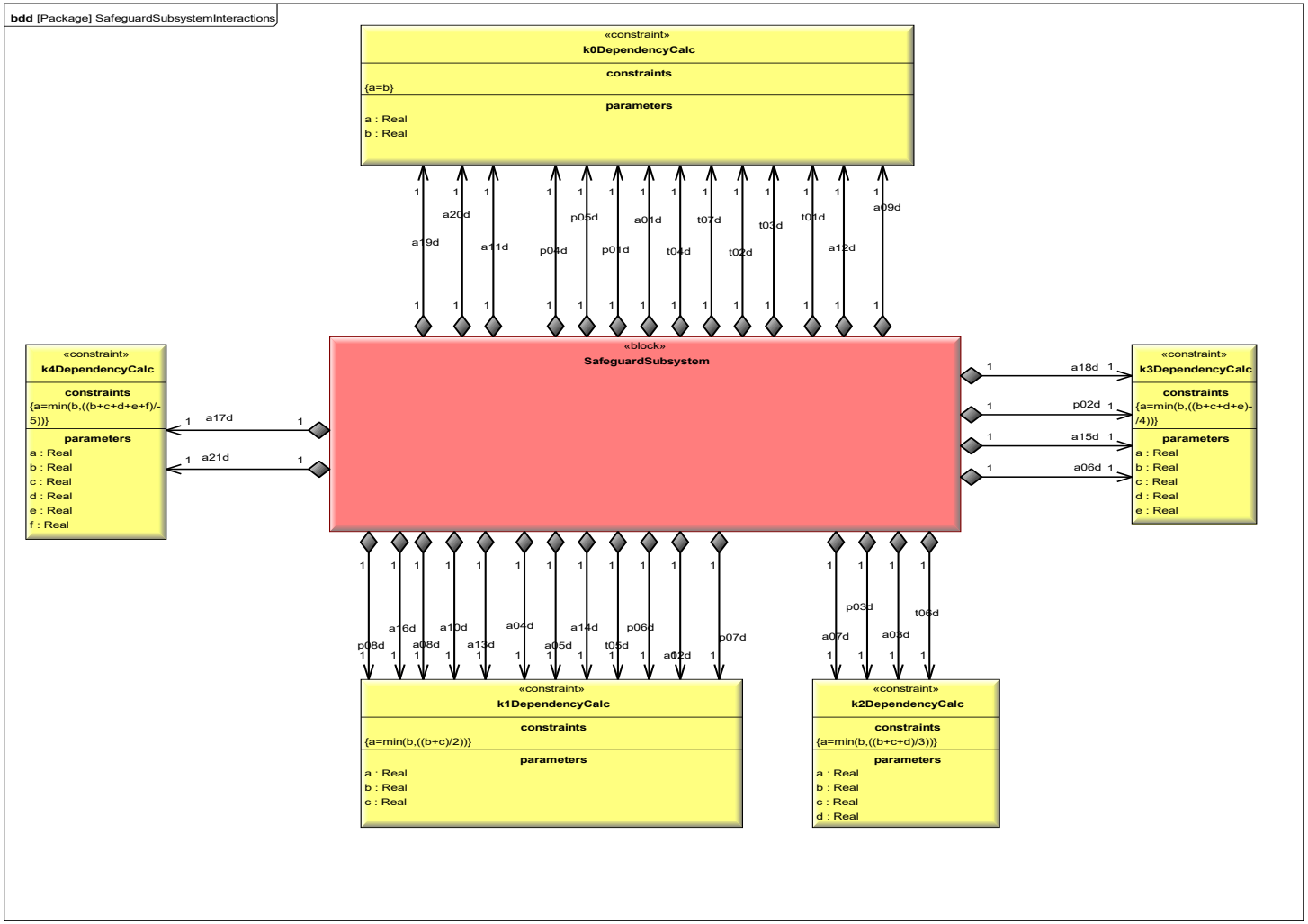
Name: [Package] Safeguard Subsystem BDD
FullScopedName: ISM.[Package] Safeguard Subsystem BDD
DynamicUmlClassName: BlockDefinitionDiagram



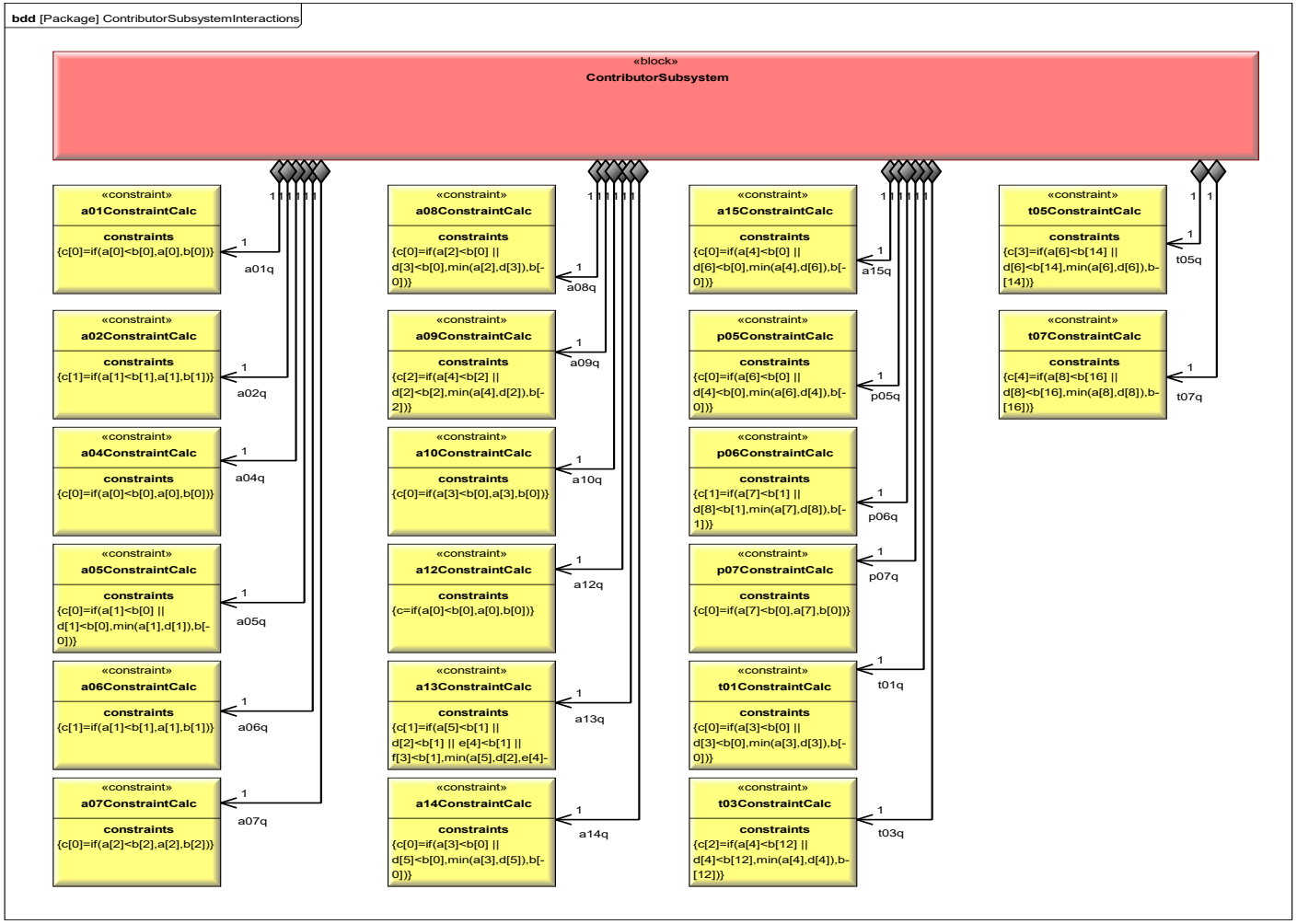
Name: [Package] Contributor Subsystem BDD
FullScopedName: ISM.[Package] Contributor Subsystem BDD
DynamicUmlClassName: BlockDefinitionDiagram



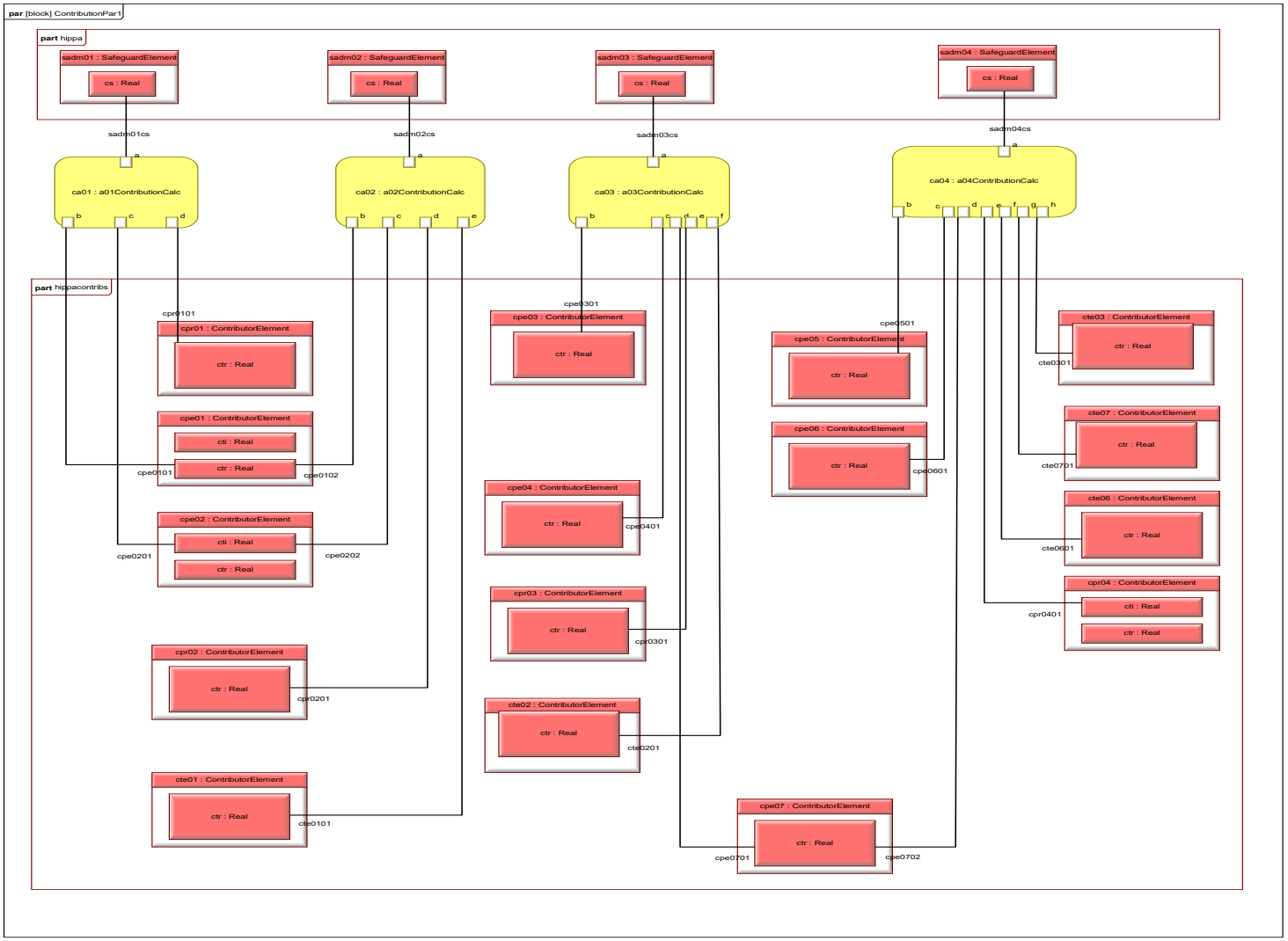
Name: [Package] ISSInteractions
FullScopedName: ISM::ISSInteractions.[Package] ISSInteractions
Description:
DynamicUmlClassName: BlockDefinitionDiagram



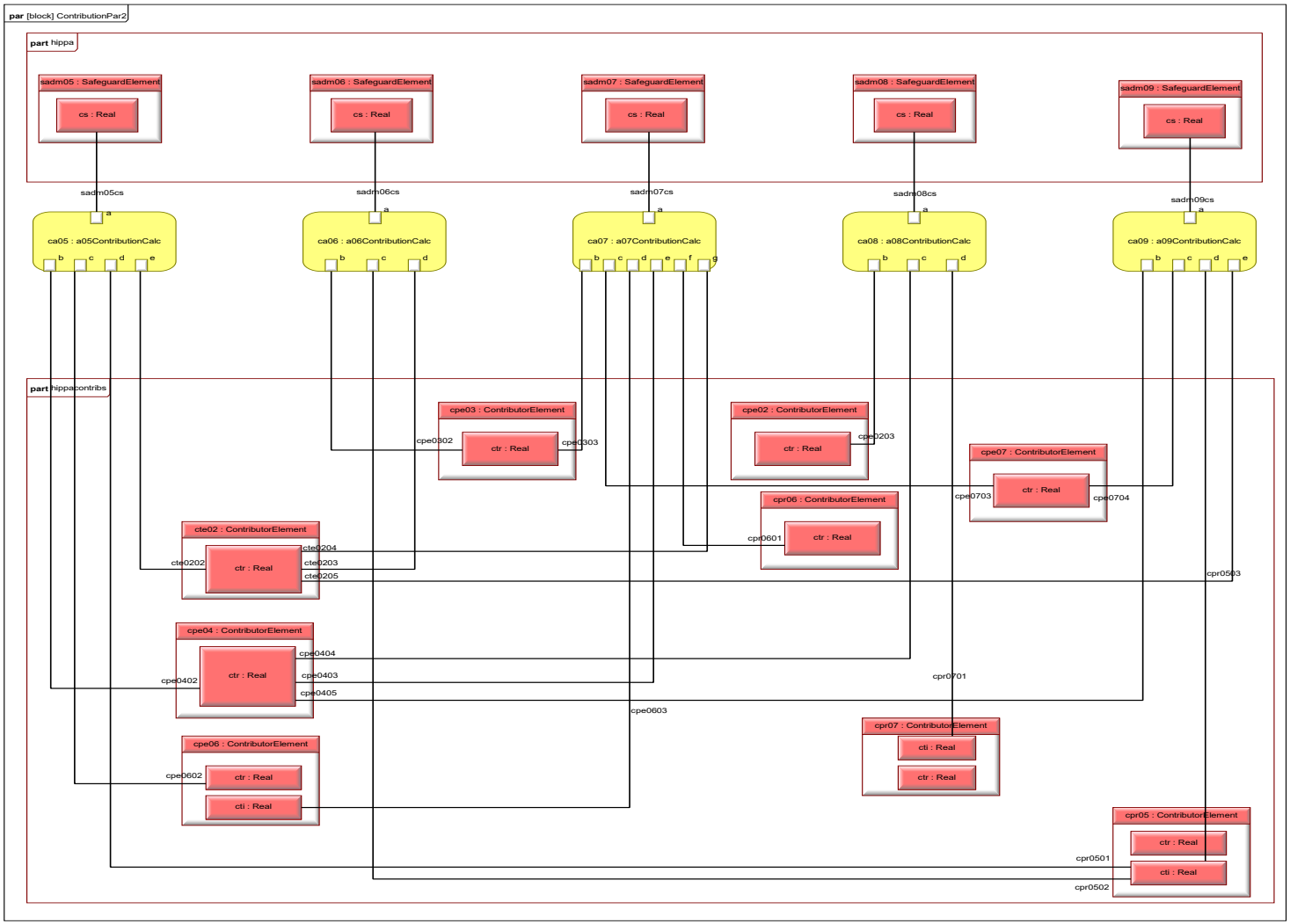
Name: [Package] SafeguardSubsystemInteractions
FullScopedName: ISM::SafeguardSubsystemInteractions.[Package] SafeguardSubsystemInteractions
DynamicUmlClassName: BlockDefinitionDiagram



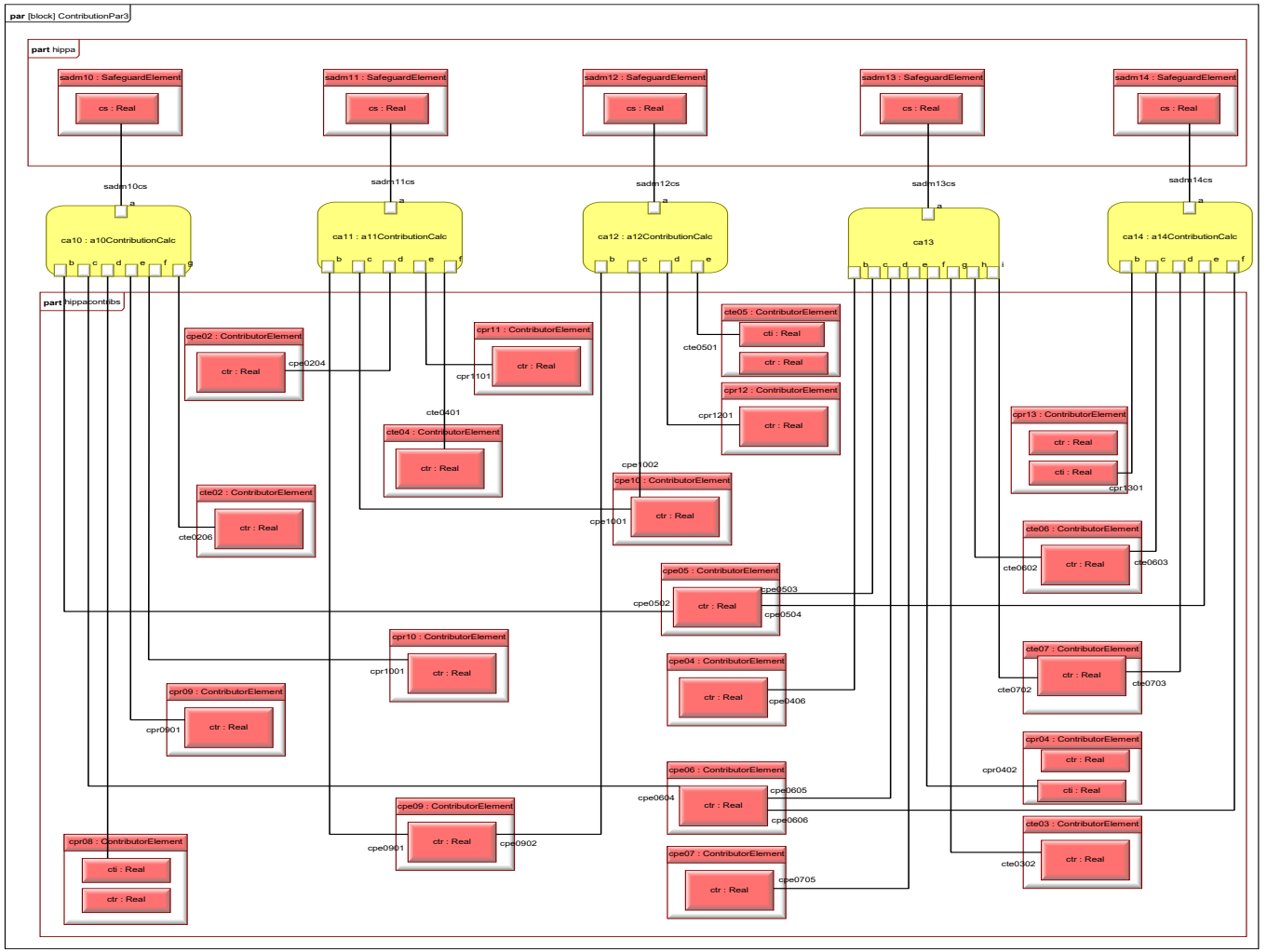
Name: [Package] ContributorSubsystemInteractions
FullScopedName: ISM::ContributorSubsystemInteractions.[Package] ContributorSubsystemInteractions
DynamicUmlClassName: BlockDefinitionDiagram



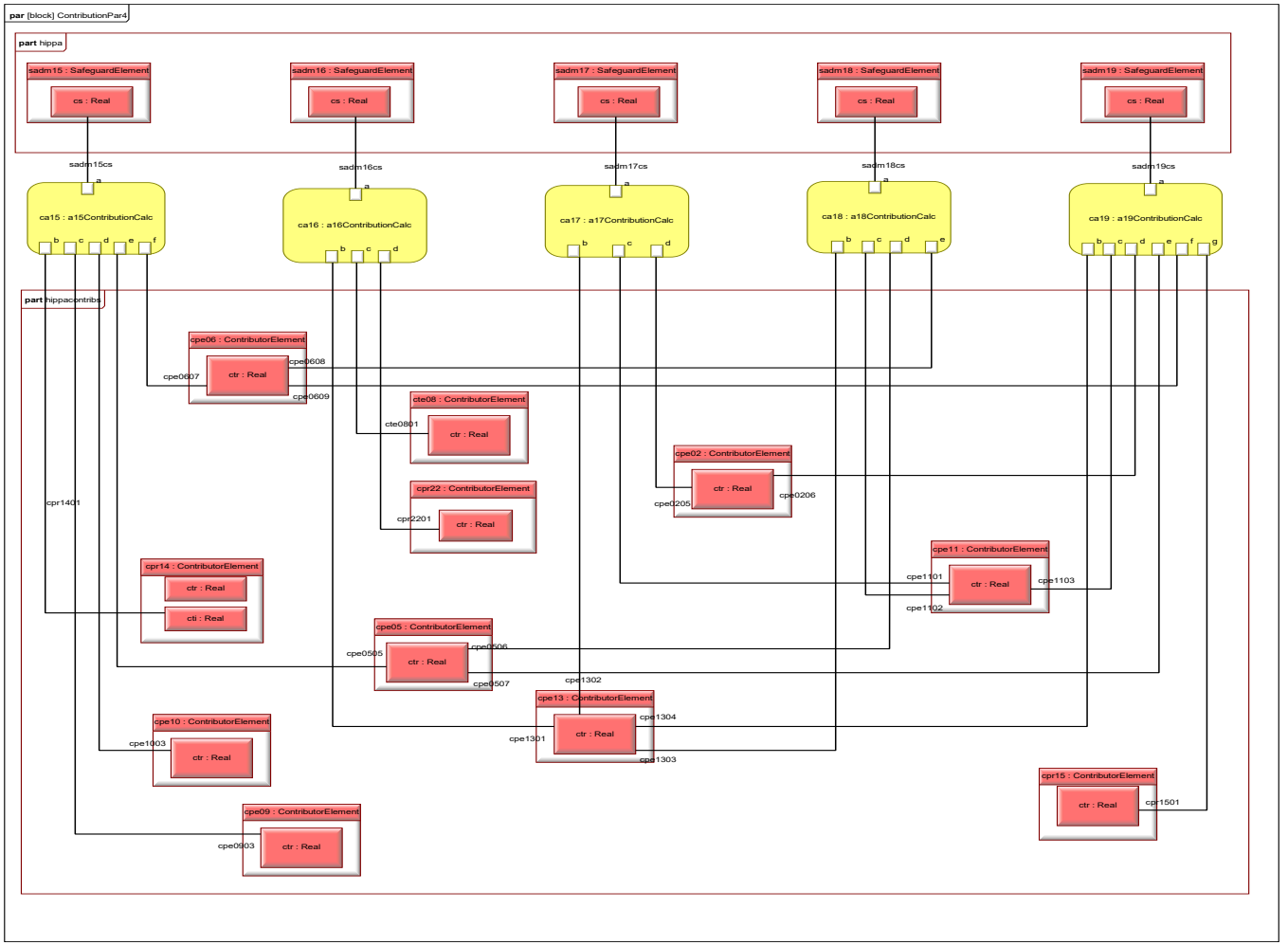
Name: [block] ContributionPar1
FullScopedName: ISM::InformationSecuritySystem.[block] ContributionPar1
DynamicUmlClassName: ParametricDiagram



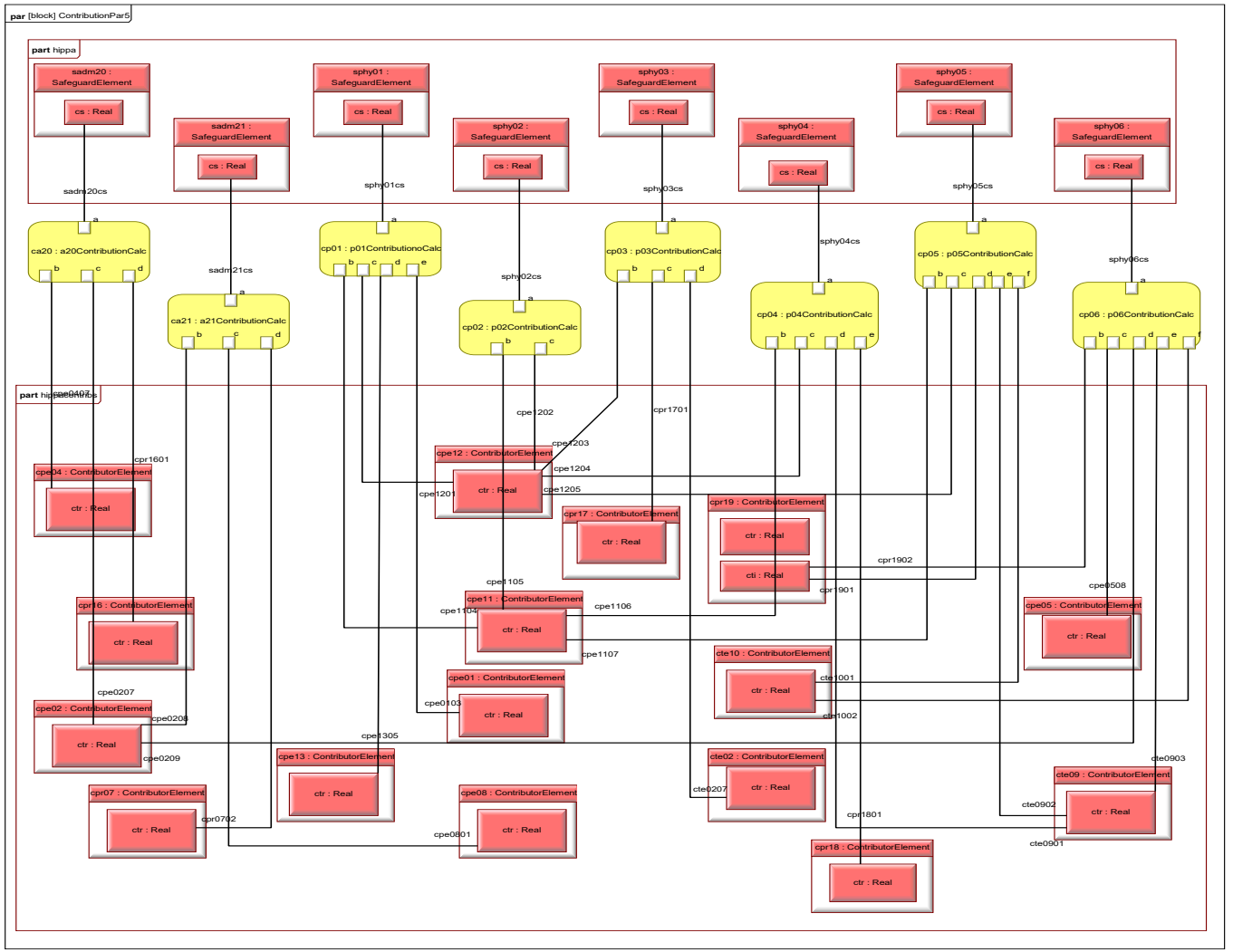
Name: [block] ContributionPar2
FullScopedName: ISM::InformationSecuritySystem.[block] ContributionPar2
DynamicUmlClassName: ParametricDiagram



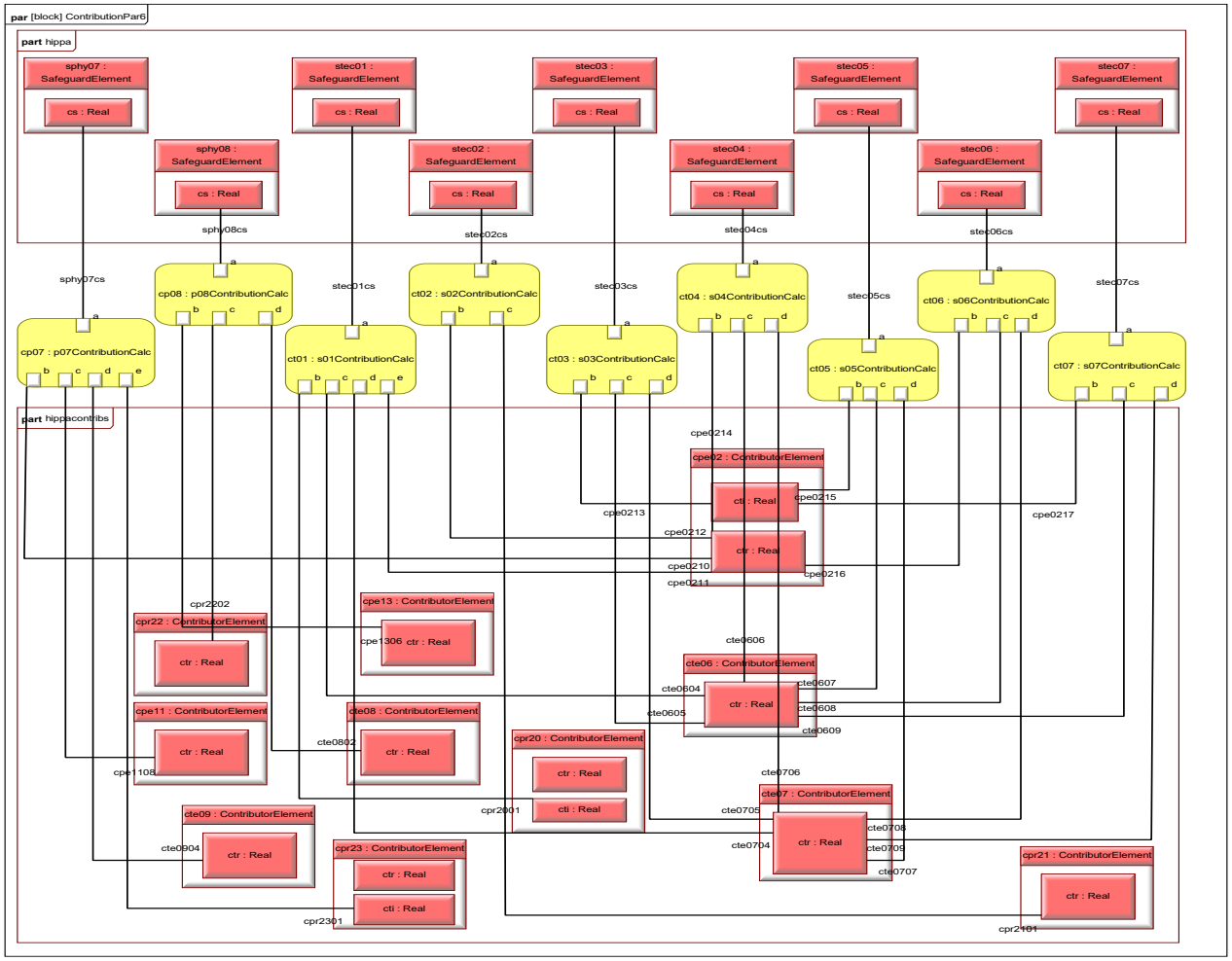
Name: [block] ContributionPar3
FullScopedName: ISM::InformationSecuritySystem.[block] ContributionPar3
DynamicUmlClassName: ParametricDiagram



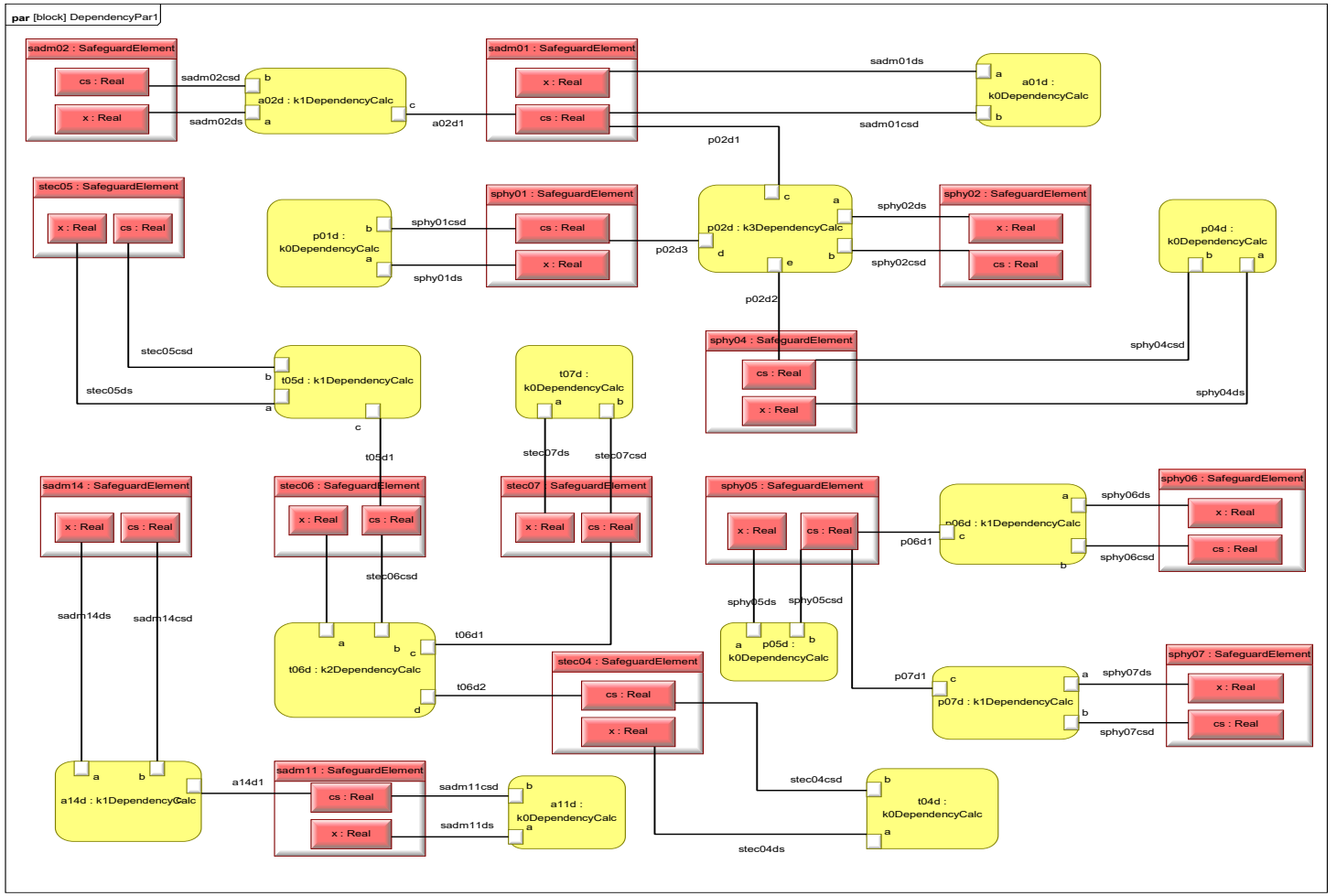
Name: [block] ContributionPar4
FullScopedName: ISM::InformationSecuritySystem.[block] ContributionPar4
DynamicUmlClassName: ParametricDiagram



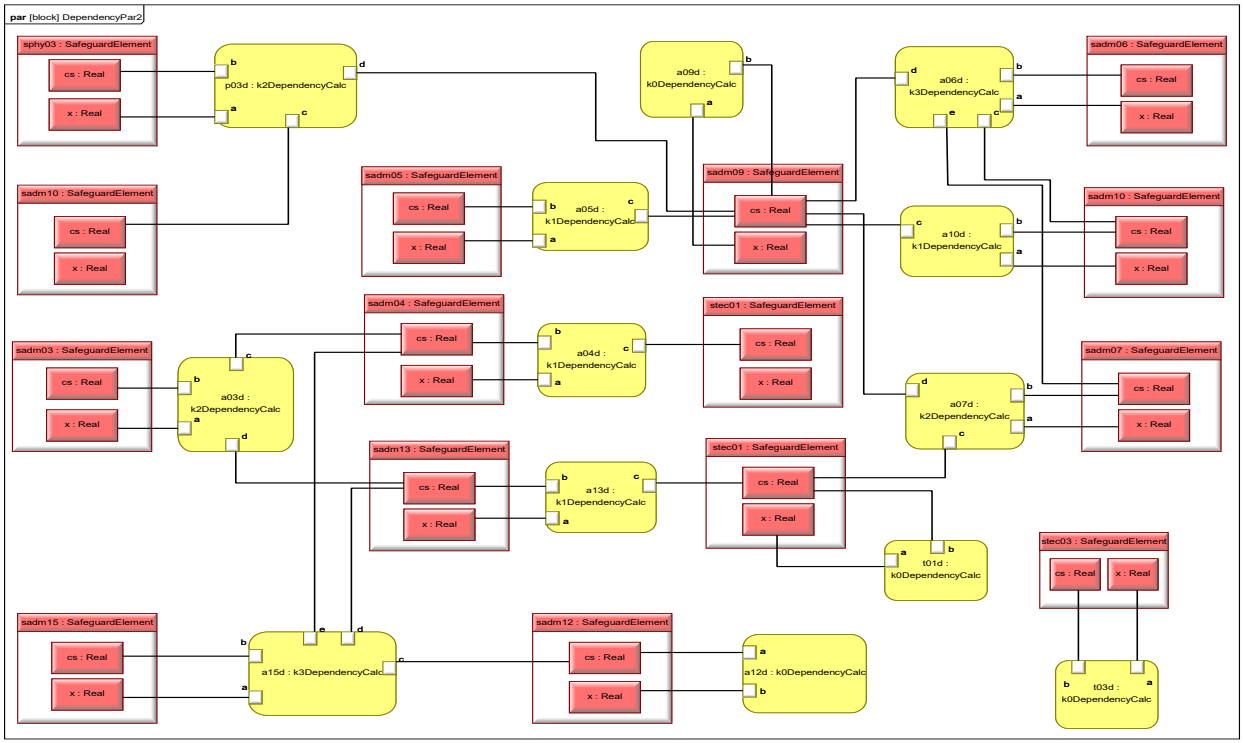
Name: [block] ContributionPar5
FullScopedName: ISM::InformationSecuritySystem.[block] ContributionPar5
DynamicUmlClassName: ParametricDiagram



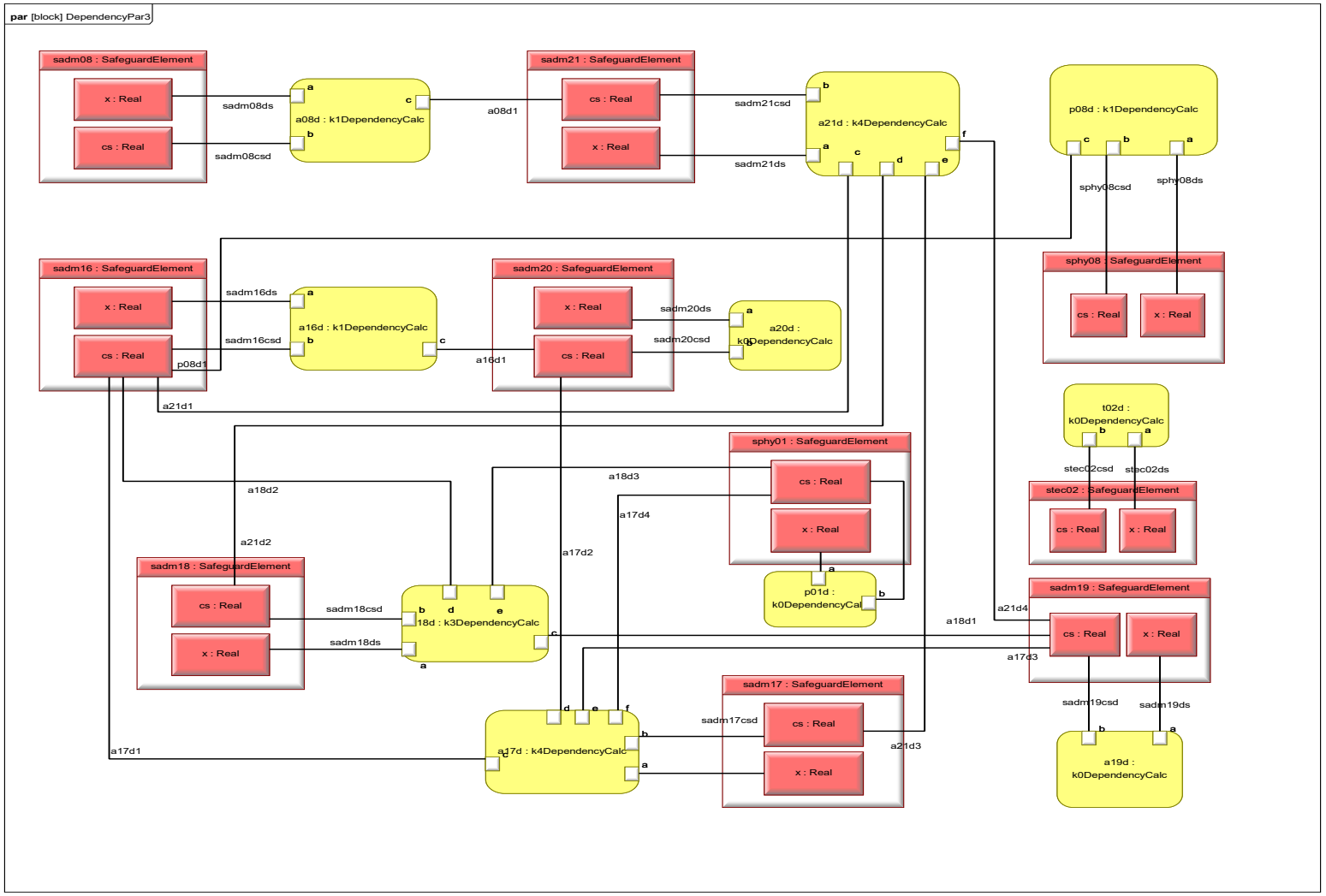
Name: [block] ContributionPar6
FullScopedName: ISM::InformationSecuritySystem.[block] ContributionPar6
DynamicUmlClassName: ParametricDiagram



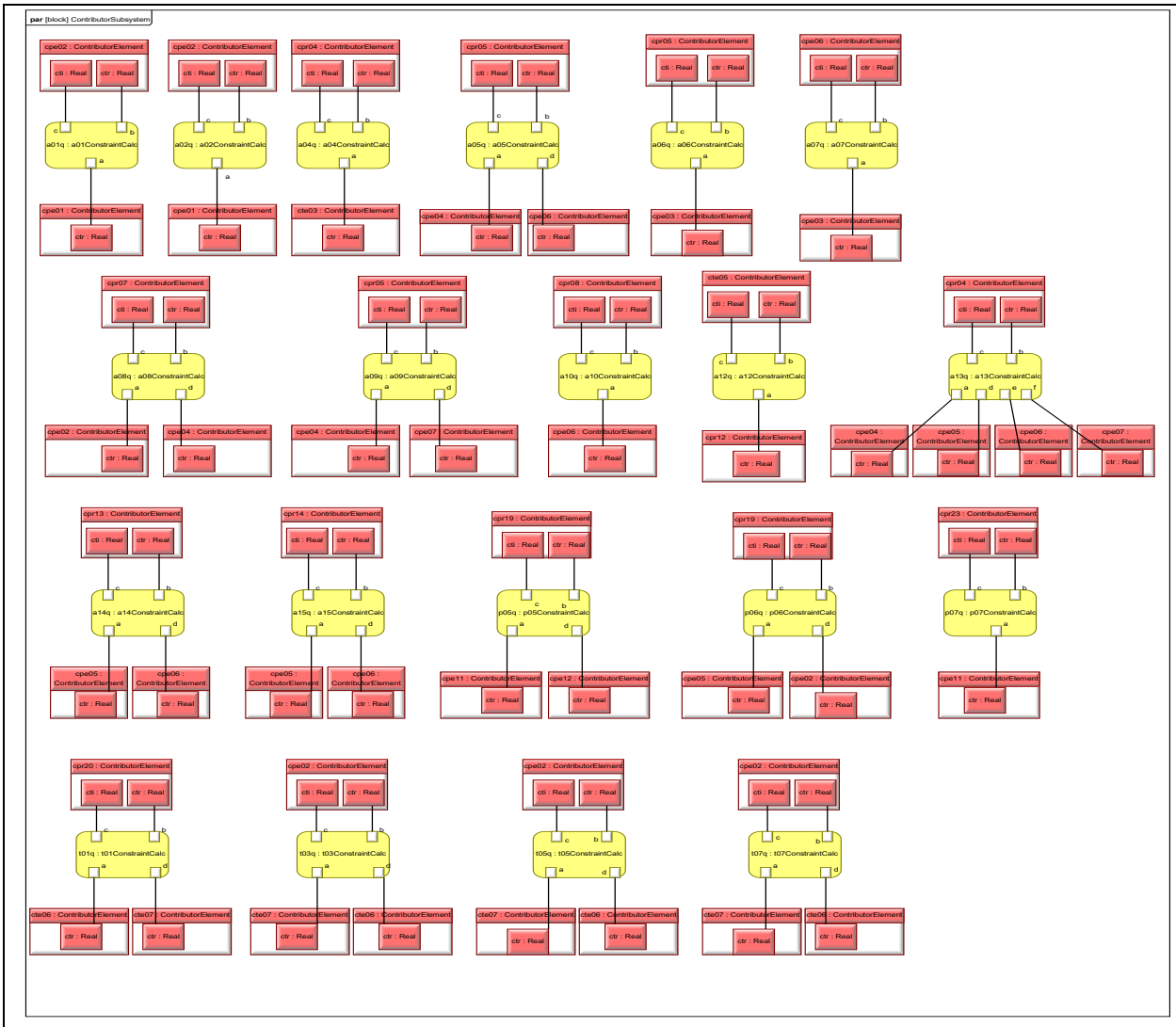
Name: [block] DependencyPar1
FullScopedName: ISM::SafeguardSubsystem.[block] DependencyPar1
DynamicUmlClassName: ParametricDiagram



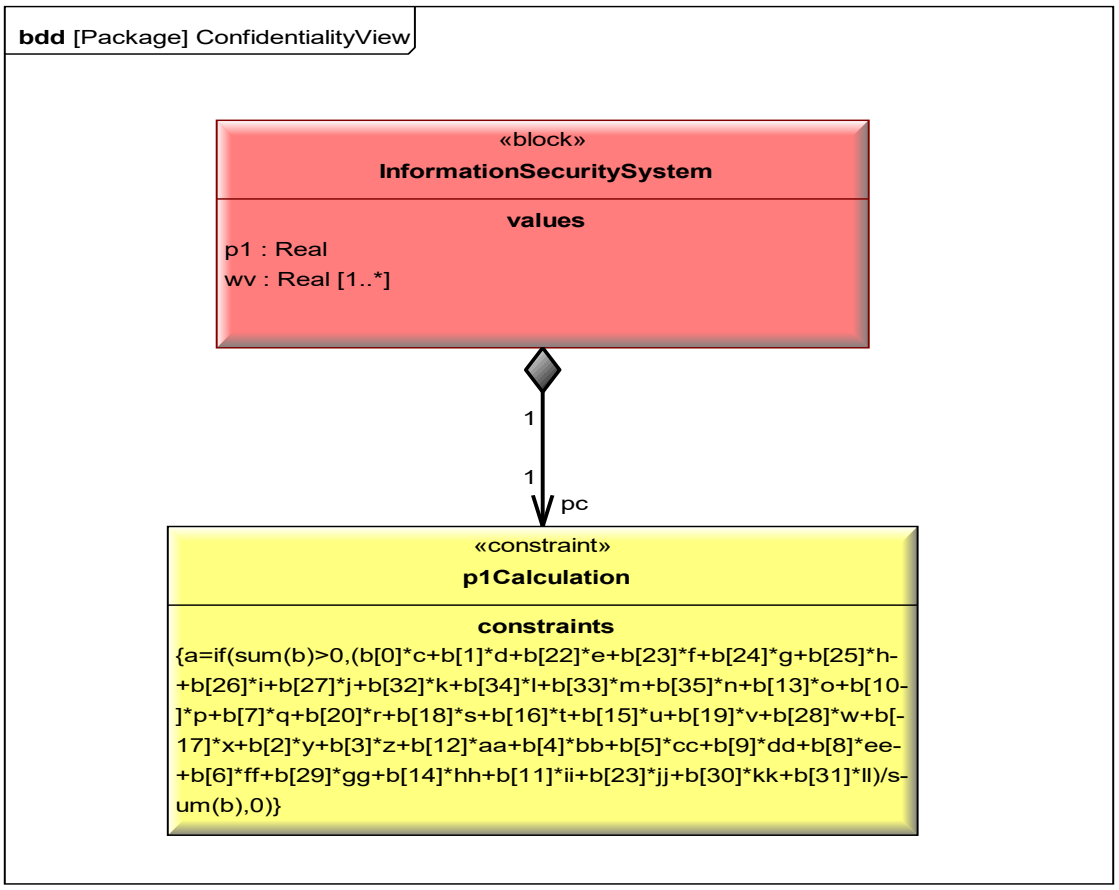
Name: [block] DependencyPar2
FullScopedName: ISM::SafeguardSubsystem.[block] DependencyPar2
DynamicUmlClassName: ParametricDiagram



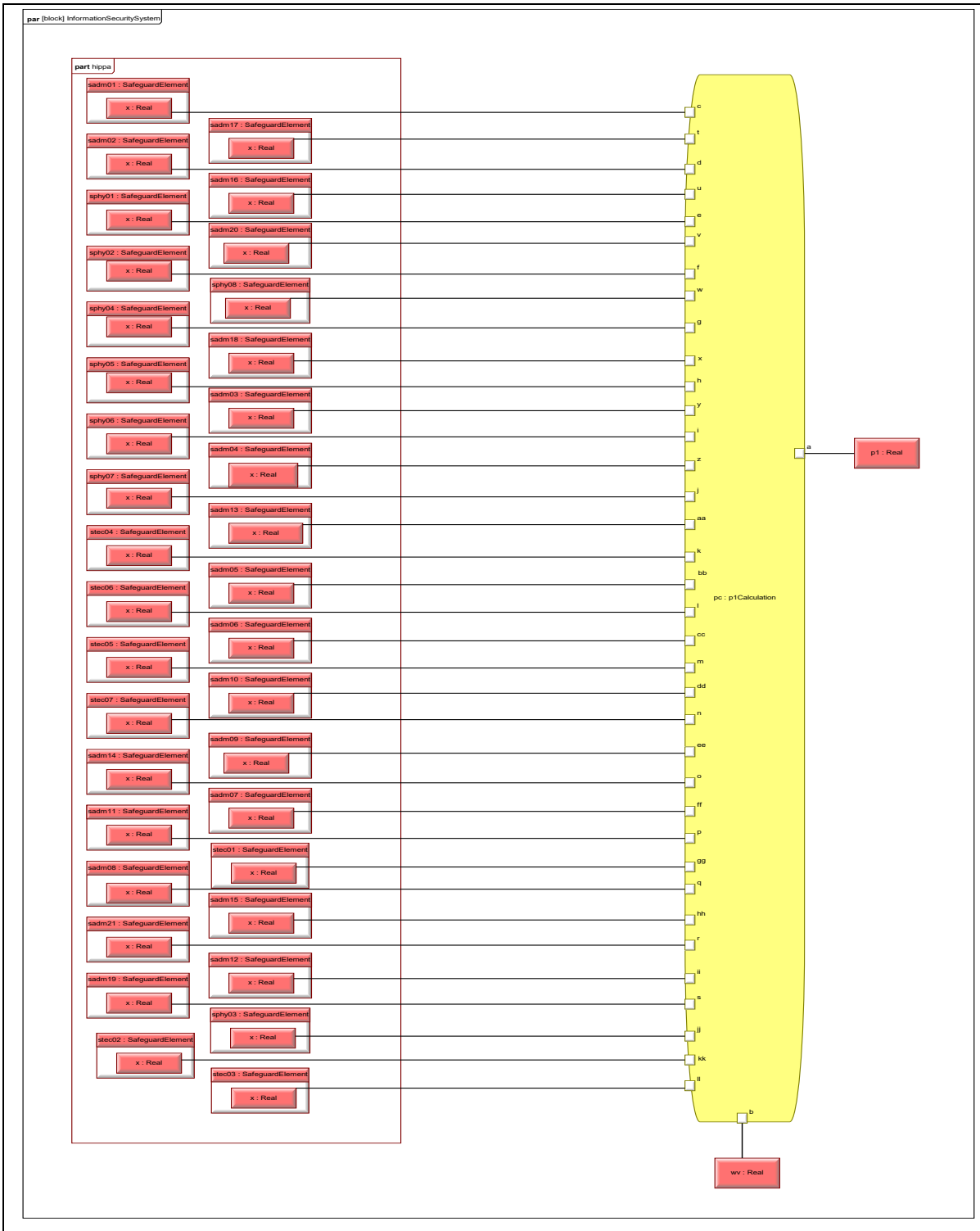
Name: [block] DependencyPar3
FullScopedName: ISM::SafeguardSubsystem.[block] DependencyPar3
DynamicUmlClassName: ParametricDiagram



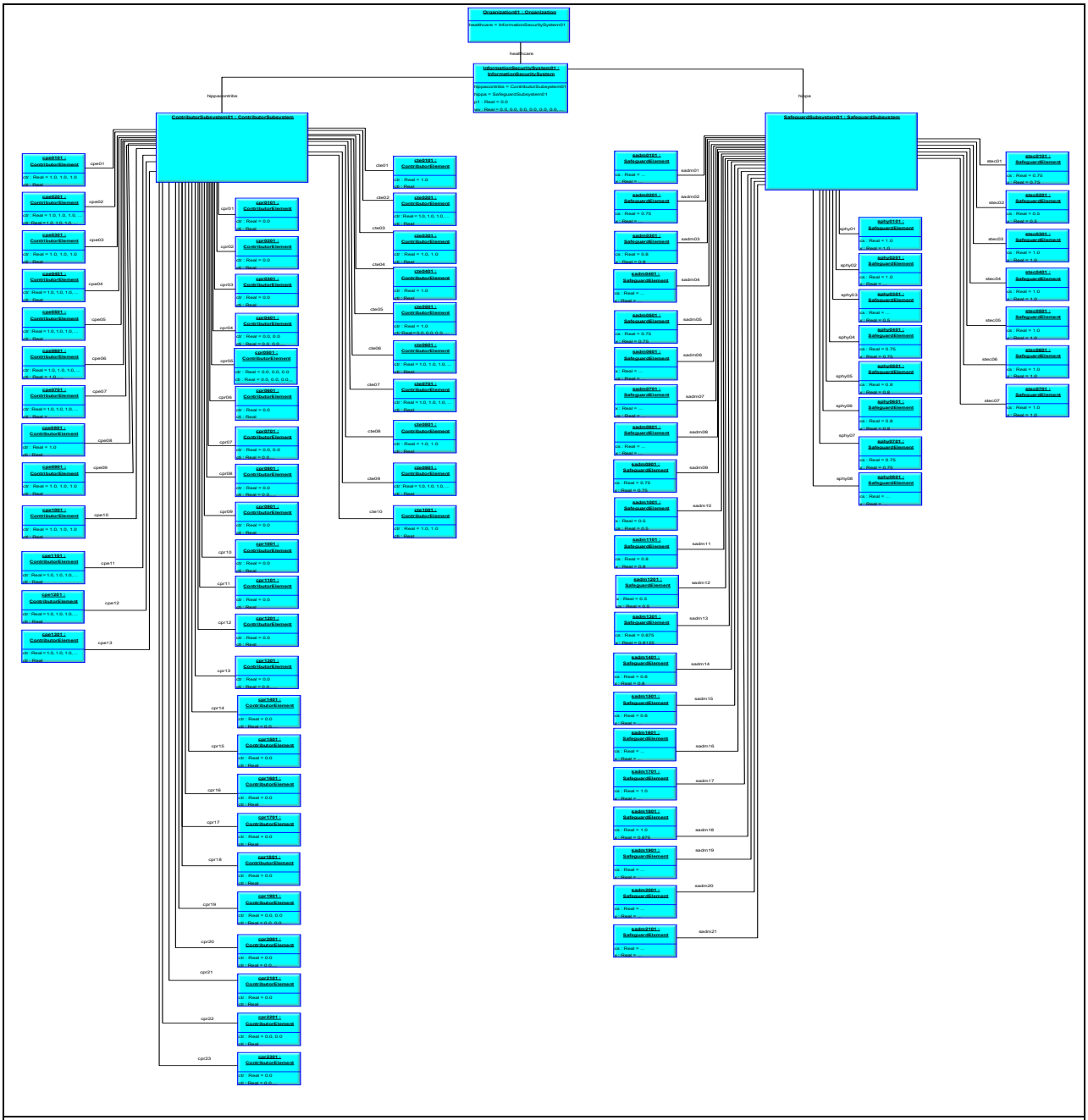
Name: [block] ContributorSubsystem
FullScopedName: ISM::ContributorSubsystem.[block] ContributorSubsystem
DynamicUmlClassName: ParametricDiagram



Name: [Package] ConfidentialityView
FullScopedName: ISM::ConfidentialityView.[Package] ConfidentialityView:
DynamicUmlClassName: BlockDefinitionDiagram



Name: [block] InformationSecuritySystem
FullScopedName: ISM::InformationSecuritySystem.[block] InformationSecuritySystem
DynamicUmlClassName: ParametricDiagram



Name: Instance01
FullScopedName: ISM::Instance01.Instance01
DynamicUmlClassName: Object Diagram

APPENDIX B: PARASOLVER OUTPUT

Verification Experiment: All ctr = 1.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	1.000	1.00	1.000	1.000
Risk Management	Administrative	S-Adm-02	1.000	1.00	1.000	
Sanction Policy	Administrative	S-Adm-03	1.000	1.00	1.000	
Information System Activity Review	Administrative	S-Adm-04	1.000	1.00	1.000	
Authorization and/or Supervision	Administrative	S-Adm-05	1.000	1.00	1.000	
Workforce Clearance Procedure	Administrative	S-Adm-06	1.000	1.00	1.000	
Termination Procedures	Administrative	S-Adm-07	1.000	1.00	1.000	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	1.000	1.00	1.000	
Access Authorization	Administrative	S-Adm-09	1.000	1.00	1.000	
Access Establishment and Modification	Administrative	S-Adm-10	1.000	1.00	1.000	
Security Reminders	Administrative	S-Adm-11	1.000	1.00	1.000	
Protection from Malicious Software	Administrative	S-Adm-12	1.000	1.00	1.000	
Log-in Monitoring	Administrative	S-Adm-13	1.000	1.00	1.000	
Password Management	Administrative	S-Adm-14	1.000	1.00	1.000	
Response and Reporting	Administrative	S-Adm-15	1.000	1.00	1.000	
Data Backup Plan	Administrative	S-Adm-16	1.000	1.00	1.000	
Disaster Recovery Plan	Administrative	S-Adm-17	1.000	1.00	1.000	
Emergency Mode Operation Plan	Administrative	S-Adm-18	1.000	1.00	1.000	
Testing and Revision Procedure	Administrative	S-Adm-19	1.000	1.00	1.000	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	1.000	1.00	1.000	
Written Contract or Other Arrangement	Administrative	S-Adm-21	1.000	1.00	1.000	
Contingency Operations	Physical	S-Phy-01	1.000	1.00	1.000	
Facility Security Plan	Physical	S-Phy-02	1.000	1.00	1.000	
Access Control and Validation Procedures	Physical	S-Phy-03	1.000	1.00	1.000	
Maintenance Records	Physical	S-Phy-04	1.000	1.00	1.000	
Disposal	Physical	S-Phy-05	1.000	1.00	1.000	
Media Re-use	Physical	S-Phy-06	1.000	1.00	1.000	
Accountability	Physical	S-Phy-07	1.000	1.00	1.000	
Data Backup and Storage	Physical	S-Phy-08	1.000	1.00	1.000	
Unique User Identification	Technical	S-Tec-01	1.000	1.00	1.000	
Emergency Access Procedure	Technical	S-Tec-02	1.000	1.00	1.000	
Automatic Logoff	Technical	S-Tec-03	1.000	1.00	1.000	
Encryption and Decryption	Technical	S-Tec-04	1.000	1.00	1.000	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	1.000	1.00	1.000	
Integrity Controls	Technical	S-Tec-06	1.000	1.00	1.000	
Encryption	Technical	S-Tec-07	1.000	1.00	1.000	

Verification Experiment: All ctr = 0.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	0.667	0.00	0.000	0.000
Risk Management	Administrative	S-Adm-02	0.708	0.00	0.000	
Sanction Policy	Administrative	S-Adm-03	0.800	0.00	0.000	
Information System Activity Review	Administrative	S-Adm-04	0.804	0.00	0.000	
Authorization and/or Supervision	Administrative	S-Adm-05	0.750	0.00	0.000	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.667	0.00	0.000	
Termination Procedures	Administrative	S-Adm-07	0.778	0.00	0.000	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	0.667	0.00	0.000	
Access Authorization	Administrative	S-Adm-09	0.750	0.00	0.000	
Access Establishment and Modification	Administrative	S-Adm-10	0.500	0.00	0.000	
Security Reminders	Administrative	S-Adm-11	0.800	0.00	0.000	
Protection from Malicious Software	Administrative	S-Adm-12	0.500	0.00	0.000	
Log-in Monitoring	Administrative	S-Adm-13	0.813	0.00	0.000	
Password Management	Administrative	S-Adm-14	0.800	0.00	0.000	
Response and Reporting	Administrative	S-Adm-15	0.758	0.00	0.000	
Data Backup Plan	Administrative	S-Adm-16	0.667	0.00	0.000	
Disaster Recovery Plan	Administrative	S-Adm-17	0.833	0.00	0.000	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.875	0.00	0.000	
Testing and Revision Procedure	Administrative	S-Adm-19	0.833	0.00	0.000	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	0.667	0.00	0.000	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.667	0.00	0.000	
Contingency Operations	Physical	S-Phy-01	1.000	0.00	0.000	
Facility Security Plan	Physical	S-Phy-02	0.854	0.00	0.000	
Access Control and Validation Procedures	Physical	S-Phy-03	0.500	0.00	0.000	
Maintenance Records	Physical	S-Phy-04	0.750	0.00	0.000	
Disposal	Physical	S-Phy-05	0.800	0.00	0.000	
Media Re-use	Physical	S-Phy-06	0.800	0.00	0.000	
Accountability	Physical	S-Phy-07	0.750	0.00	0.000	
Data Backup and Storage	Physical	S-Phy-08	0.667	0.00	0.000	
Unique User Identification	Technical	S-Tec-01	0.750	0.00	0.000	
Emergency Access Procedure	Technical	S-Tec-02	0.500	0.00	0.000	
Automatic Logoff	Technical	S-Tec-03	1.000	0.00	0.000	
Encryption and Decryption	Technical	S-Tec-04	1.000	0.00	0.000	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	1.000	0.00	0.000	
Integrity Controls	Technical	S-Tec-06	1.000	0.00	0.000	
Encryption	Technical	S-Tec-07	1.000	0.00	0.000	

Experiment: People ctr = 0.00, Process ctr = 0.00, Technology ctr = 1.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	0.000	1.00	0.000	0.238
Risk Management	Administrative	S-Adm-02	0.125	1.00	0.125	
Sanction Policy	Administrative	S-Adm-03	0.200	1.00	0.200	
Information System Activity Review	Administrative	S-Adm-04	0.429	1.00	0.429	
Authorization and/or Supervision	Administrative	S-Adm-05	0.250	1.00	0.250	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.229	1.00	0.229	
Termination Procedures	Administrative	S-Adm-07	0.167	1.00	0.167	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	0.000	1.00	0.000	
Access Authorization	Administrative	S-Adm-09	0.250	1.00	0.250	
Access Establishment and Modification	Administrative	S-Adm-10	0.167	1.00	0.167	
Security Reminders	Administrative	S-Adm-11	0.200	1.00	0.200	
Protection from Malicious Software	Administrative	S-Adm-12	0.000	1.00	0.000	
Log-in Monitoring	Administrative	S-Adm-13	0.375	1.00	0.375	
Password Management	Administrative	S-Adm-14	0.300	1.00	0.300	
Response and Reporting	Administrative	S-Adm-15	0.000	1.00	0.000	
Data Backup Plan	Administrative	S-Adm-16	0.167	1.00	0.167	
Disaster Recovery Plan	Administrative	S-Adm-17	0.000	1.00	0.000	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.000	1.00	0.000	
Testing and Revision Procedure	Administrative	S-Adm-19	0.000	1.00	0.000	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	0.000	1.00	0.000	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.000	1.00	0.000	
Contingency Operations	Physical	S-Phy-01	0.000	1.00	0.000	
Facility Security Plan	Physical	S-Phy-02	0.000	1.00	0.000	
Access Control and Validation Procedures	Physical	S-Phy-03	0.250	1.00	0.250	
Maintenance Records	Physical	S-Phy-04	0.250	1.00	0.250	
Disposal	Physical	S-Phy-05	0.400	1.00	0.400	
Media Re-use	Physical	S-Phy-06	0.400	1.00	0.400	
Accountability	Physical	S-Phy-07	0.250	1.00	0.250	
Data Backup and Storage	Physical	S-Phy-08	0.333	1.00	0.333	
Unique User Identification	Technical	S-Tec-01	0.500	1.00	0.500	
Emergency Access Procedure	Technical	S-Tec-02	0.000	1.00	0.000	
Automatic Logoff	Technical	S-Tec-03	0.667	1.00	0.667	
Encryption and Decryption	Technical	S-Tec-04	0.667	1.00	0.667	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	0.667	1.00	0.667	
Integrity Controls	Technical	S-Tec-06	0.667	1.00	0.667	
Encryption	Technical	S-Tec-07	0.667	1.00	0.667	

Experiment: People ctr = 0.00, Process ctr = 1.00, Technology ctr = 0.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	0.333	1.00	0.333	0.101
Risk Management	Administrative	S-Adm-02	0.250	1.00	0.250	
Sanction Policy	Administrative	S-Adm-03	0.067	1.00	0.067	
Information System Activity Review	Administrative	S-Adm-04	0.000	1.00	0.000	
Authorization and/or Supervision	Administrative	S-Adm-05	0.000	1.00	0.000	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.000	1.00	0.000	
Termination Procedures	Administrative	S-Adm-07	0.056	1.00	0.056	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	0.000	1.00	0.000	
Access Authorization	Administrative	S-Adm-09	0.000	1.00	0.000	
Access Establishment and Modification	Administrative	S-Adm-10	0.167	1.00	0.167	
Security Reminders	Administrative	S-Adm-11	0.200	1.00	0.200	
Protection from Malicious Software	Administrative	S-Adm-12	0.250	1.00	0.250	
Log-in Monitoring	Administrative	S-Adm-13	0.000	1.00	0.000	
Password Management	Administrative	S-Adm-14	0.000	1.00	0.000	
Response and Reporting	Administrative	S-Adm-15	0.000	1.00	0.000	
Data Backup Plan	Administrative	S-Adm-16	0.333	1.00	0.333	
Disaster Recovery Plan	Administrative	S-Adm-17	0.000	1.00	0.000	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.000	1.00	0.000	
Testing and Revision Procedure	Administrative	S-Adm-19	0.167	1.00	0.167	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	0.333	1.00	0.333	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.167	1.00	0.167	
Contingency Operations	Physical	S-Phy-01	0.000	1.00	0.000	
Facility Security Plan	Physical	S-Phy-02	0.000	1.00	0.000	
Access Control and Validation Procedures	Physical	S-Phy-03	0.222	1.00	0.222	
Maintenance Records	Physical	S-Phy-04	0.250	1.00	0.250	
Disposal	Physical	S-Phy-05	0.000	1.00	0.000	
Media Re-use	Physical	S-Phy-06	0.000	1.00	0.000	
Accountability	Physical	S-Phy-07	0.000	1.00	0.000	
Data Backup and Storage	Physical	S-Phy-08	0.333	1.00	0.333	
Unique User Identification	Technical	S-Tec-01	0.000	1.00	0.000	
Emergency Access Procedure	Technical	S-Tec-02	0.500	1.00	0.500	
Automatic Logoff	Technical	S-Tec-03	0.000	1.00	0.000	
Encryption and Decryption	Technical	S-Tec-04	0.000	1.00	0.000	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	0.000	1.00	0.000	
Integrity Controls	Technical	S-Tec-06	0.000	1.00	0.000	
Encryption	Technical	S-Tec-07	0.000	1.00	0.000	

Experiment: People ctr = 0.00, Process ctr = 1.00, Technology ctr = 1.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	0.333	1.00	0.333	0.373
Risk Management	Administrative	S-Adm-02	0.417	1.00	0.417	
Sanction Policy	Administrative	S-Adm-03	0.400	1.00	0.400	
Information System Activity Review	Administrative	S-Adm-04	0.571	1.00	0.571	
Authorization and/or Supervision	Administrative	S-Adm-05	0.250	1.00	0.250	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.333	1.00	0.333	
Termination Procedures	Administrative	S-Adm-07	0.333	1.00	0.333	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	0.000	1.00	0.000	
Access Authorization	Administrative	S-Adm-09	0.250	1.00	0.250	
Access Establishment and Modification	Administrative	S-Adm-10	0.375	1.00	0.375	
Security Reminders	Administrative	S-Adm-11	0.400	1.00	0.400	
Protection from Malicious Software	Administrative	S-Adm-12	0.500	1.00	0.500	
Log-in Monitoring	Administrative	S-Adm-13	0.375	1.00	0.375	
Password Management	Administrative	S-Adm-14	0.400	1.00	0.400	
Response and Reporting	Administrative	S-Adm-15	0.000	1.00	0.000	
Data Backup Plan	Administrative	S-Adm-16	0.500	1.00	0.500	
Disaster Recovery Plan	Administrative	S-Adm-17	0.000	1.00	0.000	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.000	1.00	0.000	
Testing and Revision Procedure	Administrative	S-Adm-19	0.167	1.00	0.167	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	0.333	1.00	0.333	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.233	1.00	0.233	
Contingency Operations	Physical	S-Phy-01	0.000	1.00	0.000	
Facility Security Plan	Physical	S-Phy-02	0.000	1.00	0.000	
Access Control and Validation Procedures	Physical	S-Phy-03	0.472	1.00	0.472	
Maintenance Records	Physical	S-Phy-04	0.500	1.00	0.500	
Disposal	Physical	S-Phy-05	0.400	1.00	0.400	
Media Re-use	Physical	S-Phy-06	0.400	1.00	0.400	
Accountability	Physical	S-Phy-07	0.250	1.00	0.250	
Data Backup and Storage	Physical	S-Phy-08	0.667	1.00	0.667	
Unique User Identification	Technical	S-Tec-01	0.750	1.00	0.750	
Emergency Access Procedure	Technical	S-Tec-02	0.500	1.00	0.500	
Automatic Logoff	Technical	S-Tec-03	0.667	1.00	0.667	
Encryption and Decryption	Technical	S-Tec-04	0.667	1.00	0.667	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	0.667	1.00	0.667	
Integrity Controls	Technical	S-Tec-06	0.667	1.00	0.667	
Encryption	Technical	S-Tec-07	0.667	1.00	0.667	

Experiment: People ctr = 1.00, Process ctr = 0.00, Technology ctr = 0.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	0.667	1.00	0.667	0.467
Risk Management	Administrative	S-Adm-02	0.500	1.00	0.500	
Sanction Policy	Administrative	S-Adm-03	0.510	1.00	0.510	
Information System Activity Review	Administrative	S-Adm-04	0.339	1.00	0.339	
Authorization and/or Supervision	Administrative	S-Adm-05	0.500	1.00	0.500	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.333	1.00	0.333	
Termination Procedures	Administrative	S-Adm-07	0.472	1.00	0.472	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	0.667	1.00	0.667	
Access Authorization	Administrative	S-Adm-09	0.500	1.00	0.500	
Access Establishment and Modification	Administrative	S-Adm-10	0.333	1.00	0.333	
Security Reminders	Administrative	S-Adm-11	0.600	1.00	0.600	
Protection from Malicious Software	Administrative	S-Adm-12	0.500	1.00	0.500	
Log-in Monitoring	Administrative	S-Adm-13	0.375	1.00	0.375	
Password Management	Administrative	S-Adm-14	0.400	1.00	0.400	
Response and Reporting	Administrative	S-Adm-15	0.557	1.00	0.557	
Data Backup Plan	Administrative	S-Adm-16	0.333	1.00	0.333	
Disaster Recovery Plan	Administrative	S-Adm-17	0.767	1.00	0.767	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.792	1.00	0.792	
Testing and Revision Procedure	Administrative	S-Adm-19	0.833	1.00	0.833	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	0.667	1.00	0.667	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.667	1.00	0.667	
Contingency Operations	Physical	S-Phy-01	1.000	1.00	1.000	
Facility Security Plan	Physical	S-Phy-02	0.792	1.00	0.792	
Access Control and Validation Procedures	Physical	S-Phy-03	0.333	1.00	0.333	
Maintenance Records	Physical	S-Phy-04	0.500	1.00	0.500	
Disposal	Physical	S-Phy-05	0.400	1.00	0.400	
Media Re-use	Physical	S-Phy-06	0.400	1.00	0.400	
Accountability	Physical	S-Phy-07	0.450	1.00	0.450	
Data Backup and Storage	Physical	S-Phy-08	0.333	1.00	0.333	
Unique User Identification	Technical	S-Tec-01	0.250	1.00	0.250	
Emergency Access Procedure	Technical	S-Tec-02	0.500	1.00	0.500	
Automatic Logoff	Technical	S-Tec-03	0.000	1.00	0.000	
Encryption and Decryption	Technical	S-Tec-04	0.333	1.00	0.333	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	0.000	1.00	0.000	
Integrity Controls	Technical	S-Tec-06	0.222	1.00	0.222	
Encryption	Technical	S-Tec-07	0.000	1.00	0.000	

Experiment: People ctr = 1.00, Process ctr = 0.00, Technology ctr = 1.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	0.667	1.00	0.667	0.773
Risk Management	Administrative	S-Adm-02	0.708	1.00	0.708	
Sanction Policy	Administrative	S-Adm-03	0.800	1.00	0.800	
Information System Activity Review	Administrative	S-Adm-04	0.804	1.00	0.804	
Authorization and/or Supervision	Administrative	S-Adm-05	0.750	1.00	0.750	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.667	1.00	0.667	
Termination Procedures	Administrative	S-Adm-07	0.778	1.00	0.778	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	0.667	1.00	0.667	
Access Authorization	Administrative	S-Adm-09	0.750	1.00	0.750	
Access Establishment and Modification	Administrative	S-Adm-10	0.500	1.00	0.500	
Security Reminders	Administrative	S-Adm-11	0.800	1.00	0.800	
Protection from Malicious Software	Administrative	S-Adm-12	0.500	1.00	0.500	
Log-in Monitoring	Administrative	S-Adm-13	0.813	1.00	0.813	
Password Management	Administrative	S-Adm-14	0.800	1.00	0.800	
Response and Reporting	Administrative	S-Adm-15	0.758	1.00	0.758	
Data Backup Plan	Administrative	S-Adm-16	0.667	1.00	0.667	
Disaster Recovery Plan	Administrative	S-Adm-17	0.833	1.00	0.833	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.875	1.00	0.875	
Testing and Revision Procedure	Administrative	S-Adm-19	0.833	1.00	0.833	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	0.667	1.00	0.667	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.667	1.00	0.667	
Contingency Operations	Physical	S-Phy-01	1.000	1.00	1.000	
Facility Security Plan	Physical	S-Phy-02	0.854	1.00	0.854	
Access Control and Validation Procedures	Physical	S-Phy-03	0.639	1.00	0.639	
Maintenance Records	Physical	S-Phy-04	0.750	1.00	0.750	
Disposal	Physical	S-Phy-05	0.800	1.00	0.800	
Media Re-use	Physical	S-Phy-06	0.800	1.00	0.800	
Accountability	Physical	S-Phy-07	0.750	1.00	0.750	
Data Backup and Storage	Physical	S-Phy-08	0.667	1.00	0.667	
Unique User Identification	Technical	S-Tec-01	0.750	1.00	0.750	
Emergency Access Procedure	Technical	S-Tec-02	0.500	1.00	0.500	
Automatic Logoff	Technical	S-Tec-03	1.000	1.00	1.000	
Encryption and Decryption	Technical	S-Tec-04	1.000	1.00	1.000	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	1.000	1.00	1.000	
Integrity Controls	Technical	S-Tec-06	1.000	1.00	1.000	
Encryption	Technical	S-Tec-07	1.000	1.00	1.000	

Experiment: People ctr = 1.00, Process ctr = 1.00, Technology ctr = 0.00						
Safeguard	**Type**	**ID**	**Dependency Score (x)**	**Confidentiality Weight (w)**	**wx**	**p1 value**
Risk Analysis	Administrative	S-Adm-01	1.000	1.00	1.000	0.659
Risk Management	Administrative	S-Adm-02	0.750	1.00	0.750	
Sanction Policy	Administrative	S-Adm-03	0.618	1.00	0.618	
Information System Activity Review	Administrative	S-Adm-04	0.339	1.00	0.339	
Authorization and/or Supervision	Administrative	S-Adm-05	0.750	1.00	0.750	
Workforce Clearance Procedure	Administrative	S-Adm-06	0.667	1.00	0.667	
Termination Procedures	Administrative	S-Adm-07	0.611	1.00	0.611	
Isolating Healthcare Clearinghouse Function	Administrative	S-Adm-08	1.000	1.00	1.000	
Access Authorization	Administrative	S-Adm-09	0.750	1.00	0.750	
Access Establishment and Modification	Administrative	S-Adm-10	0.792	1.00	0.792	
Security Reminders	Administrative	S-Adm-11	0.800	1.00	0.800	
Protection from Malicious Software	Administrative	S-Adm-12	0.750	1.00	0.750	
Log-in Monitoring	Administrative	S-Adm-13	0.438	1.00	0.438	
Password Management	Administrative	S-Adm-14	0.600	1.00	0.600	
Response and Reporting	Administrative	S-Adm-15	0.701	1.00	0.701	
Data Backup Plan	Administrative	S-Adm-16	0.667	1.00	0.667	
Disaster Recovery Plan	Administrative	S-Adm-17	0.933	1.00	0.933	
Emergency Mode Operation Plan	Administrative	S-Adm-18	0.917	1.00	0.917	
Testing and Revision Procedure	Administrative	S-Adm-19	1.000	1.00	1.000	
Applications and Data Criticality Analysis	Administrative	S-Adm-20	1.000	1.00	1.000	
Written Contract or Other Arrangement	Administrative	S-Adm-21	0.933	1.00	0.933	
Contingency Operations	Physical	S-Phy-01	1.000	1.00	1.000	
Facility Security Plan	Physical	S-Phy-02	0.938	1.00	0.938	
Access Control and Validation Procedures	Physical	S-Phy-03	0.667	1.00	0.667	
Maintenance Records	Physical	S-Phy-04	0.750	1.00	0.750	
Disposal	Physical	S-Phy-05	0.600	1.00	0.600	
Media Re-use	Physical	S-Phy-06	0.600	1.00	0.600	
Accountability	Physical	S-Phy-07	0.675	1.00	0.675	
Data Backup and Storage	Physical	S-Phy-08	0.667	1.00	0.667	
Unique User Identification	Technical	S-Tec-01	0.250	1.00	0.250	
Emergency Access Procedure	Technical	S-Tec-02	1.000	1.00	1.000	
Automatic Logoff	Technical	S-Tec-03	0.000	1.00	0.000	
Encryption and Decryption	Technical	S-Tec-04	0.333	1.00	0.333	
Mechanism to Authenticate EPHI	Technical	S-Tec-05	0.000	1.00	0.000	
Integrity Controls	Technical	S-Tec-06	0.222	1.00	0.222	
Encryption	Technical	S-Tec-07	0.000	1.00	0.000	

REFERENCES

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279-314. doi: 0.1504/IJIEM.2010.035624.

Atego (2010). Artisan Studio SysML Tutorial Version 7.2-a. Retrieved from http://www.atego.com/download-center/product-guides/

Atego Artisan Studio® (Version 7.2.23) [Software].

Atego Artisan Studio® ParaSolver (Version 7.2 R1). [Software].

Atzeni, A., Lioy, A., Gollmann, D., Massacci, F., & Yautsiukhin, A. (2006). Why to adopt a security metric? A brief survey. In Gollmann, D., Massacci, F., & Yautsiukhin, A., Quality *of Protection*. (Vol. 23, pp. 1-12): Springer US. doi: 10.1007/978-0-387-36584-8_1.

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEE Transactions on Dependable and Secure Computing*, *1*(1), 11-33. doi: 10.1109/TDSC.2004.2.

Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy*, *5*(1), 36-44. doi: 10.1109/MSP.2007.11.

Ball M. J., & Gold, J. (2006). Banking on health: personal records and information exchange. *Journal of Healthcare Information Management*, *20*(2), 71-83.

Checkland, P. (2000). Soft systems methodology: a thirty year retrospective. *Systems Research and Behavioral Science*, 17, S11-S58. doi: 10.1002/1099-1743(200011)17:1+<::AID-SRES374>3.0.CO;2-O.

Chowdhury, A., & Ray, P. (2007, June). *Privacy Management in Consumer e-Health*. Paper presented at the 9th International Conference on e-Health Networking, Application and Services. 10.1109/HEALTH.2007.381598.

Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model (Document Number CCMB-2009-07-001). (2009). Retrieved from http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Dhillon, G., & Backhouse, J. (2000). Technical opinion: information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128. doi: 10.1145/341852.341877.

Dong, C., & Dulay, N. (2006, Nov. 29 2006-Dec. 1 2006). *Privacy Preserving Trust Negotiation for Pervasive Healthcare*. Paper presented at the Pervasive Health Conference and Workshops. doi: 10.1109/PCTHEALTH.2006.361626.

Erland, J. (1998). *An integrated framework for security and dependability*. Paper presented at the 1998 Workshop on New security Paradigms (pp 22-29). doi: 10.1145/310889.310903.

Geer, D., Jr., Hoo, K. S., & Jaquith, A. (2003). Information security: why the future belongs to the quants. *IEEE Security & Privacy*, *1*(4), 24-32. doi: 10.1109/MSECP.2003.1219053.

Harris, S. (2005). All in One CISSP Exam Guide (3rd ed.). Emeryville: McGraw Hill.

Health Insurance Reform: Security Standards; Final Rule. (February 20, 2003). *Federal Register* 68(34), 8334-8381.

Hessami, A. G., & Karcanias, N. (2009, 23-26 March 2009). *Complexity, emergence and the challenges of assurance the need for a systems paradigm*. Paper presented at the 3rd Annual IEEE Systems Conference. doi: 10.1109/SYSTEMS.2009.4815779.

Hitchins, D. K. (2007). Systems Engineering: A 21st Century Systems Methodology. West Sussex: John Wiley & Sons, Ltd.

Holt, J. & Perry, S. (2008). SysML for Systems Engineering. London: The Institution of Engineering and Technology.

Hulitt, E., & Vaughn, R. B. (2008, 20-22 Oct. 2008). *Information system security compliance to FISMA standard: A quantitative measure*. Paper presented at the International Multiconference on Computer Science and Information Technology IMCSIT 2008. doi: 10.1109/IMCSIT.2008.4747334.

Hung, P. C. K. (2005*). Towards a privacy access control model for e-healthcare services*. Paper presented at the 3rd Annual Conference on Privacy, Security and Trust.

Hunstad, A., Hallberg, J., & Andersson, R. (2004, 10-11 June 2004). *Measuring IT security - a method based on common criteria's security functional requirements*. Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop. doi: 10.1109/IAW.2004.1437821.

Information Technology Security Evaluation Criteria (ITSEC). (1991). Retrieved from http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

InterCAX, LLC (2010). Artisan Studio ParaSolver™ 7.2R1 Tutorials. Retrieved from http://www-edc.eng.cam.ac.uk/~rhb24/Artisan%20Studio%20ParaSolver%20Tutorials.pdf

InterCAX, LLC (2010). Artisan Studio ParaSolver™ 7.2 R1 User's Guide.

Jahl, C. (1991). *The information technology security evaluation criteria*. Proceedings from the 13th International Conference on Software Engineering. doi: 10.1109/ICSE.1991.130656.

Keblawi, F., & Sullivan, D. (2007). The Case for Flexible NIST Security Standards. *Computer*, *40*(6), 19-26. doi: 10.1109/MC.2007.223.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509-520. doi: 10.1016/j.cose.2009.04.006.

Laprie, J. C. (1992). Dependability: Basic Concepts and Terminology: Springer-Verlag.

Laprie, J. C. (1995). *Dependable computing and fault tolerance: concepts and terminology*. Paper presented at the Twenty-Fifth International Symposium on Fault-Tolerant Computing, Highlights from Twenty-Five Years. doi: 10.1109/FTCSH.1995.532603.

LiGuo, H., Xu, B., & Suku, N. (2008). *Developing a SSE-CMM-based security risk assessment process for patient-centered healthcare systems*. Proceedings from the 6th International Workshop on Software Quality. doi: 10.1145/1370099.1370103.

Mikko, T. S., & Harri, O.-K. (2007). A review of information security issues and respective research contributions. *SIGMIS Database*, *38*(1), 60-80. doi: 10.1145/1216218.1216224.

Moore, A. P., Ellison, R. J., & Linger, R. C. (2001). Attack Modeling for Information Security and Survivability (Technical Note CMU/SEI-2001-TN-001). Carnegie Mellon University. Retrieved from http://www.sei.cmu.edu/reports/01tn001.pdf

National Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information Systems (*Federal Information Processing Standards Publication 199*)*. Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

National Institute of Standards and Technology. (2006). *Assessment of Access Control Systems* (NIST Interagency Report 7316). Retrieved from http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

National Institute of Standards and Technology. (2008). *An Introductory Resource for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security*

Rule (Special Publication 800-66). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

National Institute of Standards and Technology. (2008). *Managing Risk from Information Systems: An Organizational Perspective* (Special Publication 800-39). Retrieved from http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf

National Institute of Standards and Technology. (2009). *Directions in Security Metrics Research* (NIST Interagency Report 7564). Retrieved from http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf

National Institute of Standards and Technology. (2009). *Recommended Security Controls for Federal Information Systems and Organizations* (Special Publication 800-53). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

National Institute of Standards and Technology. (2010). *Draft Glossary of Key Information Security Terms* (NIST Interagency Report 7298). Retrieved from http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

Nicol, D. M., Sanders, W. H., & Trivedi, K. S. (2004). Model-based evaluation: from dependability to security. *IEEE Transactions on Dependable and Secure Computing*, *1*(1), 48-65. doi: 10.1109/TDSC.2004.11.

Friedenthal, S., Moore, A., & Steiner, R. (2006). Systems Modeling Language (OMG SysML™) Tutorial. Retrieved from www.omgsysml.org/INCOSE-OMGSysML-Tutorial-Final-090901.pdf

Object Management Group. (2010). OMG Systems Modeling Language (OMG SysML™) Specification, Version 1.2. Retrieved from http://www.omg.org/cgi-bin/doc?formal/10-06-02.pdf

Pfleeger, S. L., & Cunningham, R. K. Why Measuring Security Is Hard. *IEEE Security & Privacy*, *8*(4), 46-54. doi: 10.1109/MSP.2010.60.

Ritchey, R. W., & Ammann, P. (2000). *Using model checking to analyze network vulnerabilities*. Proceedings of the 2000 IEEE Symposium on Security and Privacy, pp.156-165. doi: 10.1109/SECPRI.2000.848453.

Sallhammar, K., Helvik, B. E., & Knapskog, S. J. (2006, 20-22 April 2006). *Towards a stochastic model for integrated security and dependability evaluation*. Paper presented at the First International Conference on Availability, Reliability and Security, pp. 20-22. doi: 10.1109/ARES.2006.137.

Stewart, J. M., Tittel, E., & Chapple, M. (2005). CISSP Certified Information Systems Security Professional Study Guide (3rd ed.). Alameda: SYBEX Inc.

System Security Engineering - Capability Maturity Model Security Metrics. (2011). Retrieved from http://www.sse-cmm.org/metric/metric.asp

System Security Engineering Capability Maturity Model: Model Description Document Version 3.0. (2003). Retrieved from http://www.sse-cmm.org/docs/ssecmmv3final.pdf

Tan, L., & Zhou, M.-T. (2006, Oct. 2006). *A New Evaluation Strategy Based on Combining CC and SSE-CMM for Security Systems and Products*. Paper presented at the 5th International Conference on Grid and Cooperative Computing, pp.395-403. doi: 10.1109/GCC.2006.12.

Thomas, C. R. (1997). Privacy, information technology, and health care. *Communications of the ACM*, *40*(8), 92-100. doi: 10.1145/257874.257896.

Traian Marius, T., Farshad, F., & Daniel, B.-J. (2003). *Privacy and confidentiality management for the microaggregation disclosure control method: disclosure risk and information loss measures.* Proceedings from the 2003 ACM workshop on privacy in the electronic society, pp. 21-30. doi: 1145/1005140.1005144.

Traian Marius, T., Farshad, F., & Daniel, B.-J. (2004). *Assessing global disclosure risk in masked microdata*. Proceedings from the 2004 ACM workshop on Privacy in the electronic society, pp. 85-93. doi: 10.1145/1029179.1029202.

Traian Marius, T., Farshad, F., & Daniel, B.-J. (2004). *Disclosure risk measures for the sampling disclosure control method*. Proceedings from the 2004 ACM symposium on Applied computing, pp. 301-306. doi: 10.1145/967900.967964.

Trivedi, K. S., Dong Seong, K., Roy, A., & Medhi, D. (2009, 25-28 Oct. 2009). *Dependability and security models*. Paper presented at the 7th International Workshop on Design of Reliable Communication Networks, pp.11-20. doi: 10.1109/DRCN.2009.5340029.

Truta, T. M., Fotouhi, F., & Barth-Jones, D. (2003, 9-11 July 2003). *Disclosure risk measures for microdata*. Paper presented at the 15th International Conference on Scientific and Statistical Database Management, pp. 15- 22. doi: 10.1109/SSDM.2003.1214948.

U.S. Department of Defense. (1985). Trusted Computer System Evaluation Criteria. (DoD 5200.28-STD). Retrieved from http://csrc.nist.gov/publications/history/dod85.pdf

U.S. Department of Health and Human Services. (2006). Health Information Technology Initiative Major Accomplishments: 2004-2006. Retrieved from http://www.hhs.gov/healthit/news/Accomplishments2006.html

U.S. Department of Health and Human Services Office of the Inspector General. (2011). *Nationwide Rollup Review of the Centers for Medicare and Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight* (OIG publication No. A-04-08-05069). Retrieved from http://oig.hhs.gov/oas/reports/region4/40805069.pdf

U.S. Department of Homeland Security. (2009). A Roadmap for Cyber Security Research. Retrieved from http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

U.S. Government Accountability Office. (2009). Federal *Information Systems Controls Audit Manual (FISCAM)* (GAO publication No. GAO-09-232G). Retrieved from http://www.gao.gov/new.items/d09232g.pdf

Vaughn Jr, R. B., Henning, R., & Fox, K. (2002). An empirical study of industrial security-engineering practices. *Journal of Systems and Software*, *61*(3), 225-232. doi: 10.1016/S0164-1212(01)00150-9.

Vilhelm, V. (2009). *Quantified security is a weak hypothesis: a critical survey of results and assumptions*. Proceedings of the 2009 workshop on New security paradigms, pp. 37-50. doi: 10.1145/1719030.1719036.

W. W. Stead. (2009). Electronic health records. *Information Knowledge Systems Management*, *8*(1-4), 119-143.

Wang, A. J. A. (2005). *Information security models and metrics.* Proceedings of the 43rd annual Southeast regional conference - Volume 2, pp. 178-184. doi: 10.1145/1167253.1167295.

Wang, C. & Wulf, W.A. (1997). *Towards a Framework for Security Measurement*. Paper presented at the 20th National Information System Security Conference. Retrieved from http://csrc.nist.gov/nissc/1997/proceedings/522.pdf

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4-19. doi: 10.1108/09685220910944722.

Whitmore, J. J. (2001). A method for designing secure solutions. *IBM Systems Journal*, *40*(3), 747-768. doi: 10.1147/sj.403.0747.

Winkler, W., Domingo-Ferrer, J., & Torra, V. (2004). Masking and Re-identification Methods for Public-Use Microdata: Overview and Research Problems. In Domingo-Ferrer, J. & Torra, V, *Privacy in Statistical Databases.* (Vol. 3050, pp. 519-519): Springer Berlin / Heidelberg. Doi: 10.1007/978-3-540-25955-8_17.

Wolfram Mathematica® (Version 8.0) [Software].