Discovering Multidimensional Correlations among Regulatory Requirements to Understand Risk

R. A. GANDHI, University of Nebraska, Omaha
S. W. LEE, University of North Carolina, Charlotte

Security breaches most often occur due to a cascading effect of failure among security constraints that collectively contribute to overall secure system behavior in a socio-technical environment. Therefore, during security certification activities, analysts must systematically take into account the nexus of causal chains that exist among security constraints imposed by regulatory requirements. Numerous regulatory requirements specified in natural language documents or listed in spreadsheets/databases do not facilitate such analysis. The work presented in this article outlines a stepwise methodology to discover and understand the multidimensional correlations among regulatory requirements for the purpose of understanding the potential for risk due to noncompliance during system operation. Our lattice algebraic computational model helps estimate the collective adequacy of diverse security constraints imposed by regulatory requirements and their interdependencies with each other in a bounded scenario of investigation. Abstractions and visual metaphors combine human intuition with metrics available from the methodology to improve the understanding of risk based on the level of compliance with regulatory requirements. In addition, a problem domain ontology that classifies and categorizes regulatory requirements from multiple dimensions of a socio-technical environment promotes a common understanding among stakeholders during certification and accreditation activities. A preliminary empirical investigation of our theoretical propositions has been conducted in the domain of The United States Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). This work contributes a novel approach to understand the level of compliance with regulatory requirements in terms of the potential for risk during system operation.

Categories and Subject Descriptors: D.2.1 [**Software Engineering**]: Requirements/Specifications—*Methodologies, tools*; K.5.2 [**Legal Aspects of Computing**]: Governmental Issues—*Regulations*

General Terms: Security, Measurement, Legal Aspects, Standardization

Additional Key Words and Phrases: Software requirements engineering, knowledge engineering, certification and accreditation, risk, requirements visualization, ontology-based domain modeling

ACM Reference Format:
Gandhi, R. A. and Lee, S. W. 2011. Discovering multidimensional correlations among regulatory requirements to understand risk. ACM Trans. Softw. Eng. Methodol. 20, 4, Article 16 (September 2011), 37 pages. DOI = 10.1145/2000799.2000802 http://doi.acm.org/10.1145/2000799.2000802

The work described in this article is the revised and extended version of a paper presented at the International Requirements Engineering Conference (RE'07).
This research was supported in part by the grant (Contract# N65236-05-P-3672) from the Critical Infrastructure Protection Center, Space and Naval Warfare (SPA WAR) Systems Center, US Department of Navy, Charleston, SC, and by the National Science Foundation (NSF) grant DUE: Federal Cyber Service: SFS #0416042.
S. W. Lee is now affiliated with The University of Texas, San Antonio.
David Notkin, Editor, was in charge of the review process for this article.
Authors' addresses: R. A. Gandhi, Nebraska University Center for Information Assurance, College of Information Science and Technology, University of Nebraska, Omaha, NE; email: rgandhi@unomaha.edu; S. W. Lee (corresponding author), Department of Information Systems and Technology Management, The University of Texas, San Antonio, TX; email: Seok-Won.Lee@utsa.edu.

DOI 10.1145/2000799.2000802 http://doi.acm.org/10.1145/2000799.2000802

1. INTRODUCTION

Achieving compliance with security regulations is a significant undertaking while developing and maintaining critical software systems. Organizations now perceive regulatory compliance as a primary driver of life cycle security efforts for their critical software systems and infrastructures, even surpassing worms and viruses [Ernst and Young 2005]. However, the growing number of regulations and the exhaustive process of complying with numerous regulatory security requirements pose huge costs in the government, defense and private sectors. Despite these costs, reports [Davis 2005; Ernst and Young 2005; US GAO 04-376 2004; US GAO 05-700 2005] indicate that the process of assessing compliance with regulatory security requirements is irregular and unreliable. Often infrastructure-wide standard Certification and Accreditation (C&A) processes fail to provide adequate information for authorizing officials to understand security risks and make informed decisions [US GAO 04-376 2004].

Security certification activities establish the extent to which a particular design and implementation meets a set of specified regulatory security requirements (usually referred to as baseline security controls) [DoD 5200.40 1997]. Compliance with regulatory requirements is mandatory if found applicable to the software system being certified. To consider the unique characteristics of every software system and its environment, C&A activities recommend a flexible risk-based strategy to come up with cost-effective security solutions. Following certification, the goal of accreditation activities is to agree upon an "acceptable level of risk" for authorizing system operation, as shown in Figure 1. It should be noted that the C&A process is not something that is established once to get over with; but, it is a commitment that lasts throughout the software system life cycle from inception through development and deployment to phase out [Kimbell and Walrath 2001].

During the C&A process, as shown in Figure 1, the level of compliance with regulatory requirements becomes a key input for stakeholders involved in the accreditation activities to understand the potential for "risk" during system operation. With growing software system complexity, security breaches most often occur due to a cascading effect of failure among security constraints (e.g., weakest link syndrome) that collectively contribute to overall secure software system behavior in a socio-technical environment. As a result, understanding the necessity and sufficiency of regulatory requirements and corresponding countermeasures in support of an operational environment with acceptable level of risk is not a mere checklist exercise. To understand the true potential for risk, certification analysts and accreditation officials must systematically take into account the nexus of causal chains that exist among regulatory requirements. However, numerous regulatory requirements specified in natural language documents or listed in spreadsheets/databases do not facilitate such analysis. In addition, the large collection of compliance evidence resulting from certification activities is now far beyond the capacity of manual approaches to understand the potential for risk due to noncompliance without additional representational and cognitive aids. To address these issues, the work presented in this article outlines a stepwise methodology to discover and understand the multidimensional correlations among regulatory security requirements to understand the potential for risk during system operation due to noncompliance.

"Risk" is best understood as a function of the likelihood of a future adverse event and its impact [Stoneburner et al. 2002]. The assessment of this likelihood and impact requires the consideration of a combination of extrinsic and intrinsic factors of a software system. The extrinsic factors include threat likelihood (i.e., a combination of agent, motive, means, and opportunity) and asset value (i.e., importance to stakeholders and

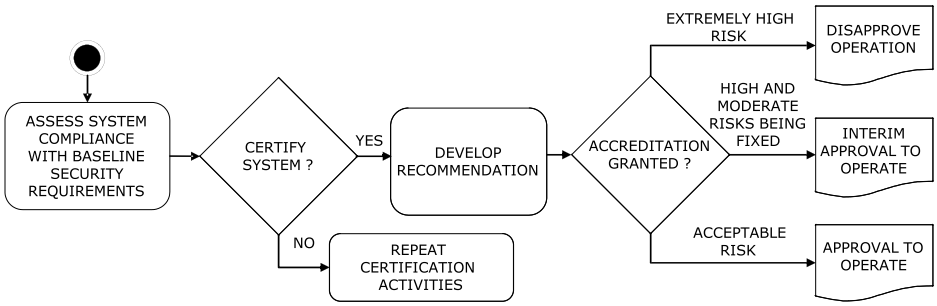

Fig. 1. Certification and accreditation activities.

impact to business/mission). The intrinsic factors include the potential of vulnerabilities (weaknesses in the system or its environment) and the collective effectiveness of installed countermeasures (i.e., constraints imposed by security requirements) to avoid vulnerabilities through systematic design practices or making them unreachable to threats. A regulatory requirements-driven approach most naturally contributes towards the understanding of the intrinsic factors, while providing implicit traceability to the extrinsic factors that motivate the applicability (and authoring) of regulatory requirements for a certain organization/business/mission. For example, the orange book [DoD 5200.28-std 1985] threat model (penetration, malicious code, and subversion) for the Department of Defense (DoD) was the basis for the corresponding evaluation criteria requirements. Particularly from an intrinsic perspective, understanding the interdependencies among constraints imposed by regulatory requirements in the operational system context is important to realize the potential for risk from a cascading failure in a complex system. Our methodology is most appealing as a starting point to later support the activities for assessing the likelihood and impact of adverse events in the system operational context. The goal is to provide initial context to reason about possible risks due to noncompliance that may eventually lead to a more comprehensive risk assessment. Our contributions towards risk assessment should be interpreted in this scope. The presented methodology does not attempt to assign values for threat likelihood, asset value, impact, vulnerability likelihood, or countermeasure costs, but provides a structured context in which such values if known could be used to rationally influence decision-making.

Our methodology relies on a requirements engineering framework to explicate regulatory requirements and related domain concepts from natural language documents and represent them using ontological domain modeling techniques [Lee et al. 2006]. The resulting Problem Domain Ontology (PDO) establishes the semantics of each requirement through its relationships with domain concepts in a socio-technical environment. Hierarchies of domain concepts in the ontology further classify and categorize requirements from multiple dimensions at different levels of abstraction. We leverage such rich conceptual understanding of regulatory requirements available from the PDO to facilitate a systematic analysis of their multidimensional correlations in the context of a software system. In a bounded scenario of investigation, conceptual overlaps among different classes of security constraints imposed by regulatory requirements are revealed based on related risk components. These conceptual overlaps are discovered and understood based on the theory of Formal Concept Analysis (FCA) [Ganter and Wille 1996] along with the domain semantics from the PDO. With analytical interventions from a certification analyst, the methodology provides

semi-automated support through an integrated requirements-driven C&A workbench [Lee et al. 2007b]. We elaborate further on the following in this article.

— To establish the semantics of security requirements based on attributes relevant to risk, we outline an explicit security requirements and risk relationship model (Section 3). The model acts as a mechanism to systematically elicit the risk components related to a security requirement specified in regulatory documents.
— To discover the multidimensional correlations among regulatory requirements for understanding the potential for risk during system operation, we discuss each step in our methodology. We use the regulatory requirements mandated by the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) [DoD 5200.40 1997] to provide illustrative examples (Section 4).
— To address the complexity of multidimensional analysis, we employ visual analytics to facilitate decision making based on evidence of non-compliance (Section 4.6). Visual metaphors derived from quantitative and qualitative metrics of requirements readily illustrate the potential for risk during system operation.
— A preliminary qualitative investigation of our theoretical propositions has been conducted in the DITSCAP domain. By gathering feedback from subject matter experts, we study how and why execution of the methodology improves the understanding of the potential for risk during system operation, given the compliance evidence from certification activities (Section 5).

2. BACKGROUND ON MODELING REGULATORY REQUIREMENTS

The regulatory security requirements provide a comprehensive coverage of security needs in the unique socio-technical environment of an organization. However, these regulatory requirements reflect the interests of multiple stakeholders in the organization who perceive risks from diverse viewpoints and at different levels of abstraction. Consequently, numerous requirements are scattered across documents originating from different levels in the organizational hierarchy without any regularity in their natural language specifications. These requirements also lack appropriate classification and categorization of the types of security constraints they enforce on system behavior. For example, some requirements impose abstract security constraints that cross-cut many aspects of system behavior, whereas other requirements mandate specific security constraints, which are applicable only in a particular instance of system design and implementation. Due to these issues, it is difficult to understand what constraints on software behavior are adequate in a given context and what level of resources should be expended upon them [US GAO 07-837 2007] for operating the system at an acceptable level of risk.

Before any meaningful analysis can be performed using regulatory security requirements, it is necessary to first identify the attributes that classify and categorize them to the dimensions which are relevant to the problem solving activity. For example, Robinson and Pawlowski [1998] use hierarchical requirements structuring and grouping for identifying conflicts. Cysneiros et al. [2004] suggest a hyperlinked lexicon representing common vocabulary in the domain to integrate nonfunctional requirements with functional design artifacts. Wasson [2006] recommends capturing various explications of concepts related to domain semantics to better manage the risk of mis-communication in requirements. Formalization of goals extracted from regulatory policies to clarify ambiguities is also suggested by Breaux et al. [2006].

In our approach, rather than relying on any single requirements modeling philosophy, we explicate each regulatory security requirement based on attributes that capture the goals, scenarios, viewpoints, and other domain-specific concepts necessary for precisely establishing their semantics. However, for requirements specified in

natural language these attributes are often missing, ambiguous or dispersed across multiple documents, limiting the use of formal approaches to process them. To address these issues, we have identified several heuristics [Lee et al. 2006] that help in eliciting these attributes present sparsely in regulatory documents by applying complementary requirements engineering techniques. Specifically, guided by the Ontology-based ACTive Requirements Engineering (Onto-ActRE) framework [Lee and Gandhi 2005], we harness the expressiveness of ontologies to classify and categorize regulatory requirements from the following dimensions: 1) a requirements domain model of security requirement types that hierarchically categorizes regulatory requirements; 2) a viewpoints hierarchy that models different perspectives and related stakeholders of a regulatory requirement; 3) a C&A process goal hierarchy and associated scenarios to express C&A process activities related to a regulatory requirement; and 4) domain-specific taxonomies of risk components of assets, threats, vulnerabilities, and countermeasures related to regulatory requirements. This representation of regulatory security requirements, using object-oriented ontological domain modeling techniques, transforms them into an interconnected web of information pieces that can be processed independent of any requirements modeling language, or analysis technique. Within this inter-connected web, the semantics of a requirement is established based on what concepts it is related to, and how it is related to those concepts.

C&A activities require evidence to be collected from the system being certified to assess its level of compliance with regulatory requirements. Therefore, for each requirement, the PDO development involves the creation of structured compliance questionnaires by a domain expert who has many years of experience performing the C&A activities. Each question has well-defined answer options that reflect ordered levels of compliance prepared from the conjunction of criteria necessary to objectively reason about the level of compliance of the target system based on responses gathered from various resources [Lee et al. 2006].

Currently, the Onto-ActRE framework has been applied to the DITSCAP by processing approximately 800 pages of regulatory documents (a representative set of DITSCAP regulatory documents). The resulting DITSCAP PDO includes 604 domain concepts that help to understand 533 C&A requirements. Although, details about building the PDO in the DITSCAP domain are described in our prior publications [Lee and Gandhi 2006; Lee et al. 2006, 2007a] in the following section we briefly elaborate on the process of analyzing a DITSCAP requirement for identifying its relationships with domain-specific risk components, which is suitable for the scope of the work presented in this paper.

3. SECURITY REQUIREMENT AND RISK COMPONENT RELATIONSHIP MODEL

Risk breaks down into three components: assets, threats, and vulnerabilities [Alberts and Dorofee 2001a]. A typical risk assessment process begins with the identification of critical assets and system characterization, followed by the enumeration of threats to those assets, and vulnerabilities that can expose assets to threats. After the analysis of existing countermeasures in place, the risk assessment process proceeds to determine the likelihood and impact of an adverse event to determine risk and finally develop recommendation to reduce risk [Stoneburner et al. 2002]. In the context of the C&A process, at the end of the certification activities, the level of compliance with regulatory requirements plays a significant role in determining the collective effectiveness (necessity and sufficiency) of the installed countermeasures in mitigating the possibility of vulnerabilities that can expose assets to threats in the system operational context. In particular, to determine the likelihood of an adverse event and its impact, the perceived threats must be analyzed in context of the potential vulnerabilities

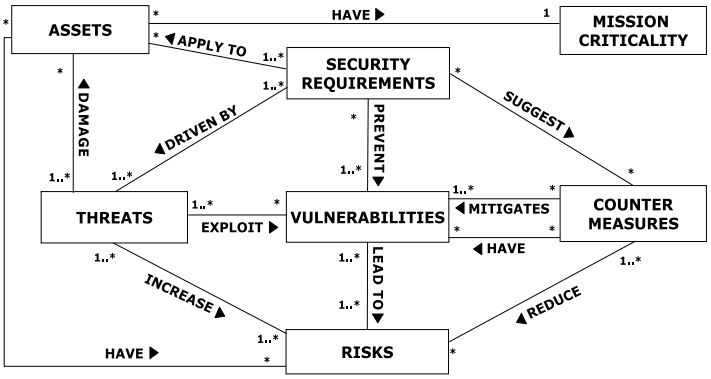

Fig. 2. Security requirements and risk components relationship model.

that can be exploited and the countermeasures in place to mitigate the vulnerabilities [Stoneburner et al. 2002]. Therefore, to systematically understand the potential for "risk" based on the level of compliance with regulatory security requirements, it is first necessary to explicate the relationships between the requirements and the risk components including the suggested countermeasures.

To systematically inquire about risk components expressed (or missing) in natural language regulatory security requirements descriptions, we extend the Common Criteria security model [Common Criteria 2006] to also include security requirements. The resulting model, as shown in Figure 2, leads to the conceptualization of a security requirement in terms of its related risk components.

Navigation of the relationships in the model of Figure 2 poses the following questions to explicate the risk components related to a security requirement.

— What threats drive the applicability of the security requirement?
— What vulnerabilities are prevented by the security requirement?
— What countermeasures are suggested by the security requirement?
— What assets does the security requirement apply to?

Applying this method to regulatory security requirements identifies the most critical risk components in an application domain, which may be explicitly or implicitly expressed by stakeholders at different levels of abstraction. We practiced this strategy in the DITSCAP domain by analyzing each of its regulatory security requirements. Based on the model in Figure 2, for each requirement, a domain expert identifies the relevant risk components and maps them to the concepts in the domain-specific taxonomies of threats, assets, vulnerabilities, and countermeasures modeled in the PDO. Processing a requirement description involves heuristics based on domain expertise, keyword analysis, regulatory document exploration, hierarchical browsing of existing concepts in the PDO and navigating their relationships. As an example, Figure 3 shows the risk components identified for the DITSCAP "Boundary Defense" requirement [Dodi 8500.2 2003]. After such processing, the discovered relationships are modeled as nontaxonomical links among security requirements and risk components in the PDO.

4. DISCOVERING MULTIDIMENSIONAL CORRELATIONS AMONG REGULATORY REQUIREMENTS TO UNDERSTAND RISK

The steps in our methodology are designed to support certification analysts in systematically estimating the collective adequacy of diverse security constraints imposed by

Requirement Name: Boundary Defense

Information Assurance Service: Confidentiality

Description: Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.

Probe Questions	Risk Components	Identification Source
What **threats** *drive* the applicability of the security requirement?	Unauthorized Internet Access	Domain Expertise
	Unauthorized Network Traffic	Domain Expertise
What **assets** does the security requirement *apply to*?	Enclave	Keyword Analysis
	DoD Information System	Keyword Analysis
What **countermeasures** are *suggested* by the security requirement?	Install Firewalls and IDS at Key points in the Enclave with appropriate configuration	Keyword Analysis
	Managed Internet Access Control Points (DMZ)	Keyword Analysis
What **vulnerabilities** are *prevented* by the security requirement?	Firewall and IDS mis-configurations	Related Countermeasure
	Internet access not proxied	Related Countermeasure
	Use of Tampered Software	Related Requirement

Fig. 3. Analyzing a DITSCAP requirement.

regulatory requirements, or lack thereof leading to potential security risks in the context of system operation. The methodology derives the semantics of security requirements from the PDO and reveals multidimensional correlations among them using the theory of Formal Concept Analysis (FCA) [Ganter and Wille 1996]. The resulting insights help an analyst establish links among security requirements from various aspects/dimensions in the context of system operation and understand the "true" extent of risks due to noncompliance. We now detail the steps in our methodology.

4.1 STEP 1: Goal-Driven Scenario Composition

The notion of "risk" being fundamentally subjective, its understanding cannot be separated from the environment in which the system operates or its purpose. Therefore, to explicitly consider system context in our methodology, we use operational scenarios as triggers for an effort to understand the potential for risk due to noncompliance. While at a broad system scope it may be difficult to enumerate possible situations that lead to risk, operational scenarios help focus on specific functionalities provided by the system. For a large and complex system, scenarios provide a situated and bounded context to map the abstract constraints specified by regulatory security requirements to their concrete implementations. During certification activities, operational scenarios can be easily elicited from domain experts and/or derived from other artifacts (e.g., use/misuse cases, system manuals, etc.) of the software system.

Evidence-based safety certification [McDermid 2001] also takes a scenario-based approach. It involves identifying potential failure modes that lead to hazards in the system context; and then, providing evidence that these failure modes are unlikely to occur or have been mitigated to an acceptable level based on safety requirements. The CORAS model-based risk assessment approach [Aagedal et al. 2002] also employs misuse case [Alexander 2003] scenarios to identify threats to the selected assets. Voas [1999] further suggests that C&A artifacts should be bound to a certain environment, which is similar to the USDA meat certification practices.

A purpose helps justify the fitness of the investigations being made. In the context of the methodology, clearly defined "goals" help justify the choice of a particular operational scenario. Therefore, in this step, scenario selection (or its composition if

none exists) is justified based on their ability to satisfy the C&A process goals. In some cases, operational scenarios of the software system can be identified first and then appropriate goals can be discovered to interpret their results in terms of the C&A process. A goal-scenario coupling provides an explicit metric for the coverage of the system operational context considered for the purpose of the C&A activities. The output of this step is a collection of scenarios identified or composed by considering the C&A process goals.

To understand each step in the methodology, consider a hypothetical situation where the DITSCAP is being applied to a software system that hosts a data repository for certain Department of Defense (DoD) missions. To satisfy the C&A process goal of "assess risks at system interfaces" [DoD 5200.40 1997], the following operational scenario is composed by the certification analyst from the remote access use-case of the software system: "The enclave boundary enables remote access for all users with appropriate authentication and identification mechanisms."

In the DoD domain, an "enclave" refers to "collection of computing environments connected by one or more internal networks. . . " [Dodi 8500.2 2003], whose examples include local area networks and the applications they host, backbone networks, and data processing centers. The "enclave boundary" refers to "the point at which an enclave's internal network service layer connects to an external network's service layer" [Dodi 8500.2 2003].

4.2 STEP 2: Forming an Analysis Pool

In this step, the investigation of potential risks is scoped based on the set of regulatory security requirements discovered to be applicable in the selected operational scenario of the software system. Essentially, each operational scenario identified in the previous step drives the formation of an *Analysis Pool*. We define the analysis pool as an exhaustive set of regulatory security requirements that collectively contribute to secure software system behavior in a given scenario.

Given numerous regulatory requirements, exhaustive coverage of their search space is important to discover requirements originating from distant sets or in different regulatory documents while populating the analysis pool. It concerns the "requirements distance" problem [Jilani et al. 2001], which is recognized as a nontrivial problem in requirements engineering that cannot be handled well through a manual inspection of several natural language regulatory documents. To address these issues, the PDO allows a combination of syntactic and semantic search strategies to discover regulatory requirements that are applicable in a given operational scenario. In particular, syntactic keyword-based techniques are used to seed the exploration of requirements at diverse points in the entire search space (i.e., the PDO); while semantic exploration-based search techniques help discover applicable requirements in close conceptual proximity from the initial seeds. Sources of keywords include goal and scenario descriptions, domain experts, or keywords based on query expansion [Lee and Rine 2004] (e.g., synonyms in regulatory documents). Exploration-based techniques leverage the conceptual proximity among requirements in the PDO; for example, sibling, parent or non-taxonomical relationships among requirement categories.

Tool support for this step in the integrated C&A workbench [Lee et al. 2007b] uses SPARQL [Prud'hommeaux and Seaborne 2006] to perform keyword-based search on the PDO. In the example scenario, keywords of "*enclave boundary*" "*remote access*" and "*authentication and identification*" are identified from the scenario description to first apply the keyword-based search strategy. An analyst examines the search results and interactively chooses only those requirements that are applicable in the scenario. This initial set of requirements is shown in Table I.

Table I. The Set of Requirements Added to the Analysis Pool by Keyword-Based Search Strategy

Requirements selected from the results of keyword-based search	Requirements Category in the PDO
EBBD-2: Boundary Defense	Enclave Boundary Defense
ECVI-1: Voice over IP	
ECI-1: Instant Messaging	
IAIA-1 Individual Identification	Authentication and Identification
IATS-1 Token and Certificate Standards	
EBPW-1 Public WAN Connection	Network/Internet Access Control
Federal Requirement: Regulate Remote Access	
EBRU-1 Remote Access for User Functions	
EBRP- Remote Access for Privileged Functions	
EBRU-1 Remote Access for User Functions	
EBRU-1 Protection of remote access mechanisms for user functions	
EBRU-1 Remote Access for User Functions use encryption	
EBRP-1 Remote Access audit trails for Privileged Functions	
DoN Requirement: Use VPN for Remote Access	

The set of requirements in the initial search results using keywords are then browsed using exploration-based search techniques of: 1) Focused hierarchical browsing (similar to file system browsing) of sibling and parent requirements; and 2) Multidimensional browsing of nontaxonomical interdependencies among requirements through related concepts in the PDO. In the example scenario, other requirements in the conceptual proximity of the requirements in Table I are now explored. For example, using the focused hierarchical browsing, it is discovered that requirements in the "Logical Access Control" category, which is parent of the "Network/Internet Access Control" category in the PDO, are also applicable in the current scenario. These requirements are added to the analysis pool, as shown in the first row of Table II.

Finally, using multidimensional browsing, the analyst explores the nontaxonomical relationships of each requirement in Table I. Such exploration includes directly related requirements; or requirements related through stakeholders in the viewpoint hierarchy, C&A process goals in the goal hierarchy, or risk components in the risk assessment taxonomy of the PDO. For example, the analyst discovers that requirements in the "Network/Internet Access Control" category are related to requirements in the "Personnel Screening" category through the Viewpoint of "System Administrator" in the viewpoint hierarchy of the PDO, and are applicable in the current scenario. After a similar discovery process, the requirements shown in rows 2 through 7 of Table II are added to the analysis pool. To demonstrate rigor in the requirements selection process, the search criteria that led to the selection of a requirement are explicitly recorded and associated with that requirement in the analysis pool.

We emphasize that the analysis pool is formed after a systematic and iterative exploration of regulatory requirements search space (based on a common understanding provided by the PDO) that spans diverse stakeholder concerns from different levels in the organization for secure system behavior in a given application domain.

4.3 STEP 3: Introducing Abstractions in the Analysis Pool

Even for a trivial scenario, the analysis pool can contain many applicable regulatory requirements. In the resulting problem space it is easy to get lost in the details of numerous individual regulatory requirements while missing the bigger picture, that is, missing the forest for the trees. Therefore, in this step we introduce abstractions in the analysis pool to reduce its cognitive burden as well as computational complexity.

Kramer and Hazzan [2006] describe the role of abstraction in software engineering, "as a cognitive means according to which, in order to overcome complexity at a

Table II. The Set of Requirements Added to the Analysis Pool by Exploration-Based Search Strategies

Requirements discovered through Exploration based search	**Requirements Category in the** PDO	**Method of discovery**
ECLP-1 Privileged accounts assigned to privileged users	Logical Access Control	"Logical Access Control" category **subsumes** "Network/Internet Access Control" Category in the Requirements Domain Model of the PDO
ECLP-1 Least privileges and Separation of duty		
ECLP-1 Privileged accounts limited to privileged functions		
DoN Requirement: Use Public Key Infrastructure		
Access Control for privileged users and IA officer	Personnel Screening	"Network/Internet Access Control" and "Personnel Screening" categories of the Requirements Domain Model are related through the **Viewpoint of "System Administrator"** in the Viewpoint hierarchy
IA Manager, IA Officer, and privileged users undergo security clearance		
ECTP-1 Audit Trail Protection	Audit Trails	"Network/Internet Access Control" and "Audit Trails" categories of the Requirements Domain Model are related through the **"requires"** relationship
ECAT-1 Audit Trail, Monitoring, Analysis and Reporting		
EBVC-1 All VPN Traffic visible to IDS	Monitoring	"Enclave Boundary Defense" and "Monitoring" categories of the Requirements Domain Model are share the **Countermeasure of "Install Firewalls and IDS at key points in the Enclave with appropriate configurations"** in the Countermeasure taxonomy
IAM, IAO and privileged users maintain knowledge of system	Security Awareness and Training	"Personnel Screening" and "Security Awareness and Training" categories of the Requirements Domain Model are related through are related through the **Viewpoints of "System Administrator", "IAO" and "IAM"** in the Viewpoint hierarchy
DoN Requirement: Privileged users require Training		
DCSR-2 Specified Robustness	Product Specification and Evaluation	"Enclave Boundary Defense" and "Product Specification and Evaluation" categories of the Requirements Domain Model are related through the **"requires"** relationship
ECCT-1 Encryption for Confidentiality	Production, I/O Controls	"Enclave Boundary Defense" and "Production, I/O Controls" categories of the Requirements Domain Model are related through the **"requires"** relationship

specific stage of a problem solving situation, we concentrate on the essential features of our subject of thought, and ignore irrelevant details." Similarly, in this step of the methodology the purpose of abstraction is to highlight the different classes of security constraints in the analysis pool and ignore the details of individual requirements. To introduce such abstractions we rely on the categorization of regulatory security requirements available through the PDO. Specifically, the requirement categories in requirements domain model of the PDO are security requirement types that hierarchically group regulatory requirements. Therefore, we abstract individual requirements to their most specific parent requirement category in the PDO to help better focus on different classes of security constraints in the analysis pool. The identified requirement categories also reveal the level of abstraction of requirements in the analysis pool. To compute the abstraction we use the *realization inference* [Baader et al. 2002], which finds the most specific parent requirement category in the PDO that a given requirement belongs to.

Requirement categories reduce complexity of the analysis pool by grouping conceptually similar requirements; however, this abstraction must still preserve the meaning of the original requirements. Therefore, to limit the interpretation of a requirement category only in terms of the requirements it abstracts in the analysis pool, the relationships of an individual requirement with other concepts in the PDO are now associated with its requirement category obtained after the abstraction process. For the purpose of understanding the potential for risk due to noncompliance, we consider only the relationships between requirements and risk components (Figure 2) in the PDO.

For the example scenario, the "Enclave Boundary Defense" requirement category is identified by the realization inference on three security requirements in the analysis pool (first three rows in Table I). As shown in row 1 of Table III, the requirement category is then associated with all the risk components identified from the PDO, which are related to the three requirements. Similarly, other requirement category profiles are created as shown in Table III.

To move between levels of abstraction, traceability is maintained between the original requirements in the analysis pool and requirement categories in the PDO. In addition, the compliance evidence gathered using questionnaires (Section 2) associated with each individual requirement can be presented as required.

4.4 STEP 4: Creating a Model of Correlations

Abstractions in the analysis pool, "profile" each requirement category from the dimensions of related risk components. Understanding the potential for risk due to noncompliance with regulatory requirements in the given scenario now requires a systematic review of these profiles. However, due to the complexity of each profile and possible multidimensional overlaps among them, the resulting correlations among requirement categories are hard to analyze without a cognitive aid. Therefore, to structure the analysis pool we construct a lattice algebraic computational model based on the mathematical theory of Formal Concept Analysis (FCA) [Ganter and Wille 1996].

FCA mathematically "formalizes" the philosophical understanding of a "concept" as a unit of thought constituted by its components: *extent* (connections to reality) and *intent* (human thinking/semantics). FCA bounds all its computations within a *formal context* such that the resulting *formal concepts* allow fixing enough references for rationally interpreting them in human communication and argumentation [Ganter and Wille 1996]. It has been shown that FCA and logic systems based on semantic networks can be connected through their conceptual structures [Wille 1997]. This aspect has been highly explored for building ontologies using concepts suggested by FCA. However, our goal here is not to compare *formal concepts* in FCA to domain concepts in the PDO. Rather, we use *formal concepts* to systematically discover and understand the multidimensional correlations among the requirements in the analysis pool. We now briefly review the theory of FCA required for the steps in the methodology.

4.4.1 An Introduction to Formal Concept Analysis. FCA defines a *formal context* as a triple: (G, M, I), where G is a set of *formal objects*; M is a set of *formal attributes*; and I is a binary relation between G and M, such that it is a subset of the Cartesian product G x M.

To understand a *formal concept*, consider the mapping functions σ and τ such that:

$$\text{For a set of formal objects } A \subseteq G, \quad \sigma(A) = \{m \in M \mid \forall g \in A : (g, m) \in I\} \tag{1}$$

$$\text{For a set of formal attributes } B \subseteq M, \quad \tau(B) = \{g \in G \mid \forall m \in B : (g, m) \in I\} \tag{2}$$

Then a formal concept "c" is defined as a pair (A, B), if and only if:

$$A = \tau(B) \wedge B = \sigma(A). \tag{3}$$

The sets A = ext (c) and B = int (c) are the mathematical derived *extent* and the *intent* of the formal concept c, respectively. Intuitively, a formal concept is a maximal collection of objects sharing common attributes. A concept $c_0 = (A_0, B_0)$ is a subconcept of concept $c_1 = (A_1, B_1)$, written as $c_0 \leq c_1$, iff:

$$A_0 \subseteq A_1 \text{ or } B_0 \supseteq B_1. \tag{4}$$

This subconcept relationship naturally corresponds to an inheritance hierarchy, where general concepts have fewer attributes than the concepts that specialize them.

Table III. Requirement Category Profiles in the Analysis Pool

Requirements Category	Threats	Assets	Countermeasures	Vulnerabilities
Enclave Boundary Defense [3-Requirements]	• Unauthorized Network Traffic • Unauthdorized Internet Access • Public IM Traffic • Public VoIP Traffic	• Enclave • DoD Information system	• Monitor installes software • Install Firewalls and IDS at key ponts in the Enclave with appropriate configurations • Managed Internet Access Control Points (DMZ)	• Configuration Vulnerability: Firewalls and IDS • Use of Tampered Software • Internet Access Not Proxied
Authentication Identification [2 Requirements]	• Unauthorized Access	• DoD Information System	• User Password Management • Key Management Procedures: Protections of Cryptographic keys • Key Management Procedures: Standards and Procedures	• Fake Certificates • Weak Key Size • Passwordbased Authentication Vulnerabilities
Network/Internet Access Control [9 Requirements]	• Unauthorized Remote Access • Unauthorized Telework Access • Unauthorized Network Traffic • Information Leak, Unauthorized Access • Data transmission Integrity Violation • Unauthorized Activities	• Enclave • DoD Information System • Remote Access Mechanisms • Audit Records • Data in transit	• Mangement Internet Access Control Points (DMZ) • Mobile Computing and Teleworking Management • VPN for Remote Access • Encryption • Key Management Procedures: Standards and Procedures • Logging and Reviewing Events	• Internet Access Not Proxied • Compromised Remote Access Terminals • VPN without Blocking Mode • Fake Certificates • Weak Key Size • IA Policy Violations
Logical Access Control [4 Requirements]	• Unauthorized Access • Employee-related Unauthorized Activities	• DoD Information System	• Privilege Mangement • Personnel Screening • Key Management Procedures: Protection of Cryptographic keys • Key Mangement Procedures: Standards and Procedures	• Excess privileges • Conflict of Interests • Insufficient Background Checks • Fake Certificates • Weak Key Size
Personnel Screening [2 Requirements]	• Employee related Unauthorized Activities	• Enclave • DoD Information System • Hardware • Software • Firmware • Data • Control Information	• Personnel Screening • Privilege Mangement	• Insufficient Background Checks • Excess Privileges
Audit Trial [2 Requirements]	• Unauthorized Activities • Data at Rest Integrity Violation	• Audit Records • DoD Information Systems	• Logging and Reviewing Events	• IA Policy Violations
Security Awareness and Training [2 Rquirements]	• Untrained Personnel	• Enclave • DoD Information Systems	• Information Security Education and Training	• Lack of Training
Product Specification and Evaluation [1 Requirement]	• Data transmission Integrity Violation	• Data in transit	• Use Certified COTS IA and IA enabled products • Encryption • Key Mangement Procedures: Standards and Procedures	• Use of Tampered Software • Fake Certificates • Weak Key Size
Production and I/O Controls [1 Requirement]	• Data transmission Integrity Violation	• Data in transit	•Encryption	• Fake Certificates • Weak Key Size

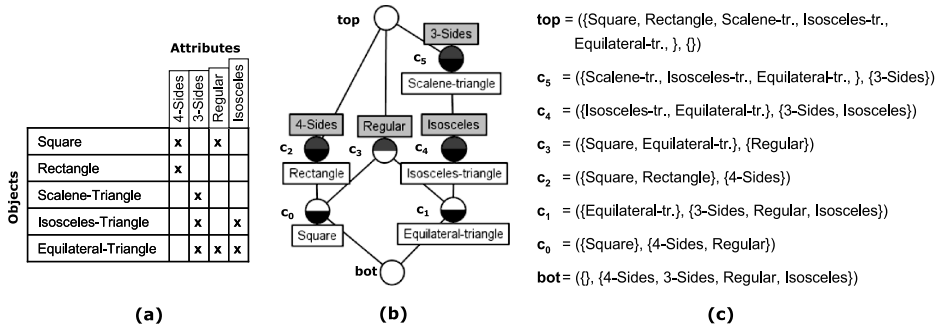

Fig. 4. (a) Example of a formal context; (b) concept lattice; and (c) formal concepts.

The subconcept relation forms a complete partial order over the set of all formal concepts and is represented as a complete lattice structure called the *concept lattice*.

A concept lattice allows two basic algebraic operations on formal concepts. For any arbitrary set of formal concepts, the *Supremum* (sup) operation gives the "least common superconcept" (least upper bound); and the *Infimum* (inf) operation gives the "greatest common subconcept" (largest lower bound) in the lattice. They are defined as follows.

$$\sup_{i\in I}(A_i, B_i) = (\tau(\cap_{i\in I} B_i), \cap_{i\in I} B_i). \tag{5}$$

$$\inf_{i\in I}(A_i, B_i) = (\cap_{i\in I} A_i, \sigma(\cap_{i\in I} A_i)). \tag{6}$$

Intuitively, the supremum is the lowest common node in the concept lattice that can be reached from all the selected formal concepts via ascending paths (intersection of intents). Similarly, the infimum is the highest common node in the concept lattice that can be reached via descending paths from all the selected formal concepts (intersection of extents).

Every formal object is associated with a unique formal concept, called the *object concept*. Similarly, every formal attribute is associated with a unique *formal concept*, called the *attribute concept*. For a concept lattice L and formal concepts $\mathsf{c} \in \mathsf{L}$ they are computed as follows:

$$\text{For } \mathsf{g} \in \mathsf{G}, \text{ the } \textit{object concept}, \ \gamma(\mathsf{g}) = \inf(\{\mathsf{c} \in \mathsf{L} \mid \mathsf{g} \in \text{ext}[\mathsf{c}]\}) \tag{7}$$

$$\text{For } \mathsf{m} \in \mathsf{M}, \text{ the } \textit{attribute concept}, \ \mu(\mathsf{m}) = \sup(\{\mathsf{c} \in \mathsf{L} \mid \mathsf{m} \in \text{int}[\mathsf{c}]\}). \tag{8}$$

The concept lattice becomes less cluttered by labeling the formal concepts only with their uniquely associated formal objects and formal attributes. An example formal context, formal concepts, and concept lattice are shown in Figure 4(a), (b), and (c) respectively (adapted from Tonella [2005]). For a node in the concept lattice of Figure 4(b), the extent of the corresponding formal concept includes all the formal objects that are reachable by navigating downward (including the selected node); and its intent includes all the formal attributes reachable by navigating upward (including the selected node).

4.4.2 Constructing the Formal Context to Understand the Potential for Risks. FCA primitives based the notion of object-attribute pairs, provides a lot of flexibility in their use and interpretation [Kalfoglou et al. 2004]. To precisely understand where to apply FCA and how to interpret its findings to understand the potential for risk due to non-compliance, we consult the model in Figure 2. Using FCA, each relationship between entities in the security requirements and risk component in Figure 2 can be studied individually

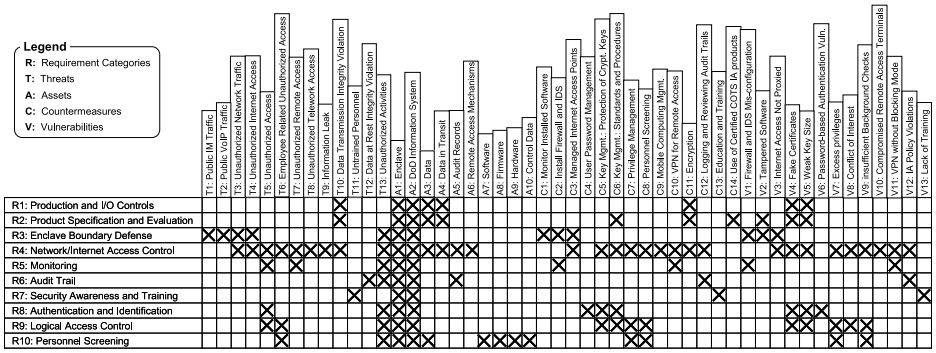

Fig. 5. Formal context for the requirements-driven risk assessment case.

or collectively as a chain of causal relationships. To understand risk, we study the relationships collectively based on the following case.

— Investigate the collective effectiveness of Security Requirements in "suggesting" Countermeasures to "mitigate" the Vulnerabilities that can be "exploited" by Threats to "damage" Assets.

To study this case using FCA, the subject of investigation is modeled as the set of formal objects; other entities related to the subject of investigation are modeled as the set of formal attributes; and their relationships are modeled as the formal context relation (crosses). The resulting formal concepts are then interpreted based on a chain of relationships supported by the model in Figure 2. We achieve this flexibility in interpretation only because the relationships among entities being studied in a case and their relationships in the PDO are derived from the same conceptual model (Figure 2).

To represent the profiles in Table III for this case, requirement categories are interpreted as the set of formal objects; their related risk components as the set of formal attributes; and their relationships (e.g., *driven_by* {C&A requirement category, Threat}) are recorded as crosses in the formal context relation. For the example scenario, the Network/Internet Access Control requirement category forms a formal object, its related risk components (as shown in Table III) form the formal attributes, and their relationships are depicted as crosses in the formal context relation. Similarly, by adding the rest of the other requirement categories and related risk components from Table III, the resulting formal context is shown in Figure 5. It should be noted that, Figure 5 also includes additional relationships between requirement categories and risk components that are discovered through operations discussed in Section 4.4.3.

The possible correlations among different classes of requirement categories now become immediately apparent from the dimensions of various risk components.

4.4.3 Augmenting the Formal Context. A requirement category profile in Table III has been constructed primarily from the representation of individual regulatory requirements in the PDO, which lack understanding about the hierarchical relationships between requirement categories as well as risk components. Therefore, there is a need to augment the formal context relation derived entirely from instance space of the PDO with what is known about the requirement categories and risk components in the conceptual space of the PDO. The hierarchical relationships can be inferred from the PDO, but the formal context relation has already been used to represent the nonhierarchical relationships between requirements and risk components. Hence, we must augment the formal concept relation I of the formal context (G, M, I) to I in a way that it also

accounts for their hierarchical relationships in the PDO. To perform this augmentation, we must first identify the mathematical constraints necessary for the hierarchical partial order among formal concepts which are uniquely associated with formal objects and attributes (Equations (7) and (8)) to preserve the hierarchical relationships among requirement categories and risk components in the PDO.

As a formal object, if a requirement category "g_1" is a subclass of another requirement category "g_2" (expressed as subclass (g_1, g_2)) in the analysis pool, then for the partial order among their uniquely associated formal concepts to respect this relationship, the infimum of all the formal concepts that contain g_1 in their extent should be a subconcept of the infimum of all the formal concepts that contain g_2 in their extent. This can be formally expressed using (7) as follows:

$$\text{subclass}\ (g_1, g_2) \wedge (g_1, g_2 \in G) \ \rightarrow \ \gamma\ (g_1) \leq \gamma\ (g_2). \tag{9}$$

From (4) it follows that after augmentation this constraint must be preserved:

$$\text{int}\ (\gamma\ (g_1)) \ \supseteq \ \text{int}\ (\gamma\,(g_2)). \tag{10}$$

To preserve (10), the augmentation procedure needs to explicitly account for the implicit risk components traceability assumed while authoring regulatory requirements. A requirement (e.g., requirements in the Network/Internet Access Control category) that specializes more general requirements (e.g., requirements in the Logical Access Control category), often either does not maintain explicit traceability to risk components specified in the parent requirements or expresses the risk components using more specific terminology. Therefore, a requirement category in the formal context is augmented with relationships to all the risk components that its parent requirement category is related to. As a result, the risk components associated with more general requirement categories in the analysis pool are explicitly considered while assessing the level of compliance in their subclass requirement categories in the analysis pool. This constraint is introduced in the formal context based on the following augmentation rule: Given $g_1, g_2 \in G, m \in M$

$$\text{subclass}\ (g_1, g_2) \wedge ((g_2, m) \in I) \ \rightarrow \ ((g_1, m) \in I^{+}). \tag{11}$$

In the context of our example, since the requirement category of Network/Internet Access Control is a subclass of "Logical Access Control" in the PDO, based on (11), the former is augmented with relationships to all risk components that the latter relates to. As a result, the vulnerability of Excess Privileges (and other risk components) related to Logical Access Control is now explicitly considered while evaluating the level of compliance with requirements in the Network/Internet Access Control category.

The augmentation process works slightly different for risk components. As a formal attribute, if a risk component m_1 is a subclass of another risk component m_2 (expressed as subclass (m_1, m_2)) in the analysis pool, then for the partial order among their uniquely associated formal concepts to respect this relationship, the supremum of all the formal concepts that contain m_1 in their intent should be a subconcept of the supremum of all the formal concepts that contain m_2 in their intent. This can be formally expressed using (8) as:

$$\text{subclass}\,(m_1, m_2) \wedge (m_1, m_2 \in M) \ \rightarrow \ \mu\ (m_1) \leq \mu\ (m_2). \tag{12}$$

From (4) it follows that after augmentation this constraint must be preserved:

$$\text{ext}\,(\mu\,(m_1)) \subseteq \text{ext}(\mu\,(m_2)). \tag{13}$$

To preserve (13), the augmentation procedure needs to explicitly account for the implicit requirements traceability assumed while authoring regulatory requirements. A requirement that refers to risk components (e.g. Data in Transit) that specialize more

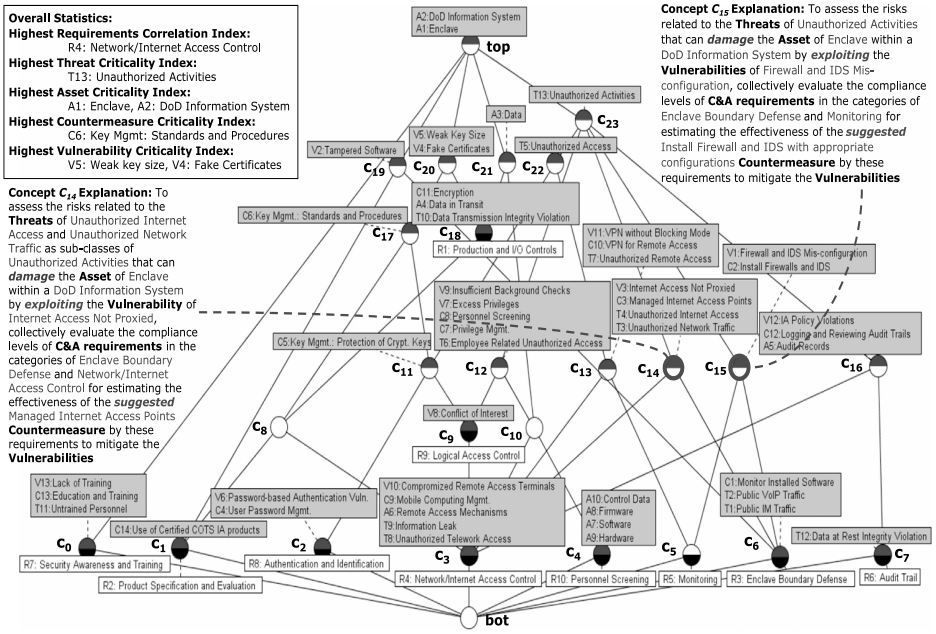

Fig. 6. Concept lattice for the formal context in Figure 5.

general risk components (e.g. "Data"), often either does not maintain traceability to the requirements that refer to the parent risk components or expresses the requirements using more specific terminology. Therefore, a risk component in the formal context is augmented with relationships to all the requirement categories that its subclass risk components are related to. As a result, the level of compliance of requirement categories associated with specific risk components in the analysis pool is explicitly considered in the context of their parent risk components in the analysis pool. This constraint is introduced in the formal context based on the following augmentation rule: Given $m_1, m_2 \in M, g \in G$

$$\text{subclass}\ (m_1, m_2) \wedge ((m_1, g) \in I) \ \rightarrow \ ((m_2, g) \in I^+). \tag{14}$$

In the context of our example, since the risk component of Data in Transit is a subclass of "Data" in the Asset taxonomy of the PDO, based on (14), all requirement categories related to the former are augmented with relationships to the latter. As a result, the level of compliance of requirements in the categories of Network/Internet Access Control, Product Specification and Evaluation, and Production and I/O Controls related to Data in transit are now explicitly considered while assessing risks to Data.

In effect, augmentation rules use domain semantics available from the PDO to reveal the true extent of the potential risks due to noncompliance. The formal context shown in Figure 5 includes the relationships discovered by applying the augmentation rules.

4.4.4 Understanding the Concept Lattice. After augmentation, the formal concepts computed from the formal context in Figure 5 are visualized as a concept lattice in Figure 6.

The concept lattice provides a compact and visual representation to discover and understand all potential correlations among requirement categories, while facilitating their interpretation in terms of the potential for risk during system operation. Each formal concept in the lattice helps to understand the potential for risk based on

requirement categories in its extent and meaningful combinations of risk components in its intent. Essentially, in the given scenario, to understand the potential for risk due to a combination of risk components within the intent of a formal concept, it is "necessary and sufficient" to collectively evaluate the compliance levels of the requirements abstracted by the requirement categories in the extent. It should be noted that the concept lattice is "minimal", such that the combinations of risk components in the intent of the formal concept are all valid with respect to the requirement categories in the extent.

A simple object-attribute pairing in the *formal context* relation flattens the semantics of the relationships between requirement categories and risk components; that is, the relationships "*driven_by*," "*prevents*," "*suggests*" and "*apply_to*" are all recorded using a cross in the formal context relation and it is no longer possible to distinguish them. Therefore, while interpreting a formal concept these semantics are restored based on the requirements and risk relationship model in Figure 2, to construct natural language explanations. Such explanations of formal concepts "C14" and "C15", as shown in Figure 6, are automatically generated by interpreting their intents and extents based on the model in Figure 2. The explanations also account for the hierarchical relationships among requirement categories as well as risk components in the PDO.

4.5 STEP 5: Risk Metrics and Measures

The lattice algebraic operations upon formal concepts support the development of several intuitive metrics to understand the potential for risk due to noncompliance. We first discuss the set of metrics that convey the range of possible risks due to simultaneous noncompliance with multiple regulatory requirements. Essentially we identify the risk upper bound and lower bound in terms of the maximum and minimum number of security constraints, respectively, that can be bypassed due to a cascading effect of noncompliance.

— *Risk upper bound upon failure in the security constraints imposed by any arbitrary number of chosen requirement categories*. It is identified by computing the supremum (Equation (5)) of the *formal concepts* that are uniquely associated with the chosen requirement categories (Equation (7)). Risk components in the intent of the supremum express the upper bound of risk. Requirement categories in the extent of the supremum express the maximum number of security constraints that can be bypassed due to a cascading effect of noncompliance.
— *Risk lower bound upon failure in the security constraints imposed by any arbitrary number of chosen requirement categories*. It is identified by computing the infimum (Equation (6)) of the formal concepts that are uniquely associated with the chosen requirement categories (Equation (7)). Risk components in the intent of the infimum express the lower bound of risks. Requirement categories in the extent of the infimum express the minimum number of security constraints that can be bypassed due to a cascading effect of noncompliance.

The risk upper bound can be visually computed by first selecting the nodes in the concept lattice that are uniquely associated with the requirement categories being investigated (Equation (7)). For example, to examine the risk upper bound of the requirement categories of Enclave Boundary Defense, Monitoring, and Network/Internet Access Control, we select the nodes C6, C5, and C3, which are labeled with them respectively. The risk upper bound is then the lowest common node reachable via ascending paths from all the selected nodes, which is node C23. The intent of node C23 conveys the risk upper bound as the Threat of "Unauthorized Activities" to the Assets of Enclave within the DoD Information System. The set of requirement categories in its extent: Logical

Access Control, Authentication and Identification, Personnel Screening, Audit Trails, Enclave Boundary Defense, Monitoring, and Network/Internet Access Control express the maximum number of security constraints that can be potentially bypassed due to a cascading effect of non-compliance. To visually compute the risk lower bound, we identify the highest common node reachable via descending paths from all the selected formal concepts. In the above case, the risk lower bound is the "bottom" concept, which is undefined because it does not have any requirement categories in its extent.

These metrics can help identify the critical risk components that can be later considered for an in-depth assessment of the likelihood and impact of adverse events in the system operational context. For example, based on the severity and likelihood of risk components associated at these conceptual bounds, appropriate mitigation strategies can be planned to localize the effect of failure. While presenting these metrics to nonexperts, generic concepts can be mapped to real world entities. For example, the asset of Data in Transit can be mapped to Secret Policies and the threat of Data transmission Integrity Violation can be mapped to Hackers of Foreign Countries in a certain operational scenario. In this manner, the methodology can be most useful when used as a precursor to a risk assessment process in the system operational context.

The C&A process deals with assets at different levels of criticality by adjusting the applicability of regulatory requirements and having different levels of rigor in performing the certification activities. For example, the DITSCAP has four different levels of rigor in the certification activities namely: (1) Minimal Security Checklist; (2) Minimum Analysis; (3) Detailed Analysis; and (4) Extensive Analysis. The System (or asset) characteristics such as interfacing mode, mission-reliance, availability, integrity, information categories, etc. determine the level of effort to be selected as well as the applicability of regulatory requirements. As different requirements become applicable, the methodology will produce different results. For example, if a less critical system is being certified, fewer and less stringent requirements will be applicable as compared to those for a highly critical system. Essentially, requirements applicability and the expected rigor in demonstrating compliance will naturally regulate the scope of the risks perceived during system operation.

A second set of metrics are derived from the concept lattice to prioritize requirement categories and risk components in the analysis pool.

— *Requirement Category Correlation Index*. It is the ratio of the number of formal concepts that include the requirement category in their extent, and the total number of formal concepts. In the range of [0, 1], higher the index of a requirement category, higher is its potential for correlation with other requirement categories.
— *Risk Component Criticality Index*. It is the ratio of the number of formal concepts that include the risk component in their intent, and total number of formal concepts. In the range of [0, 1], higher the index for a risk component, higher is its dependency on the collective compliance in many requirement categories. This index is maintained for each type of risk component.

Such prioritization metrics are highly relevant to treat security as an emergent property of the system as a whole. Based on these metrics, the most critical requirement categories and risk components identified for the example scenario are shown in Figure 6.

Finally, a metric for risk coverage in a given scenario based on the level of compliance with requirements is derived from the implications rules among risk components. Similar to functional dependencies in relational databases, implications among risk components that are satisfied by the formal context relation can be computed. Denoted as $X \rightarrow Y$, an implication holds among risk components in a formal context if

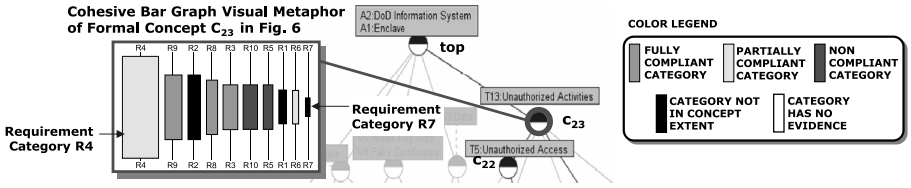

Fig. 7. Cohesive bar graph visual metaphor.

every requirement category related to all risk components in the set X, is also related to the risk components in set Y. Although the number of possible implications can be very large, a stem base [Duquenne and Davis 2005] with the fewest number of implications exists from which all other implications can be derived. The stem base is sound, complete and nonredundant. These properties allow establishing the following metric.

— *Mathematical Risk Coverage*. If all requirement categories in the analysis pool are fully compliant, then the stem base suggests that all valid implications among risk components are covered in the given scenario (100% mathematical risk coverage). On the other hand, for any noncompliant requirement categories, a subset of implications in the stem base can be identified. Then, based on implication inference (Armstrong's axioms [Armstrong et al. 2002]) a closed set of all implications that follow can be computed syntactically.

4.6 STEP 6: Enabling Insights for Decision Making

Equipped with the concept lattice and available metrics, requirements compliance levels can be visualized to directly perceive patterns and derive insights about risk during system operation. The goal of such visual analytics [Wong and Thomas 2004] is to combine human intuition with mathematically derived visual metaphors to facilitate decision making in a large information space. Therefore, to visualize the potential for risk due to noncompliance in a given scenario, we create metaphors with visual features (e.g., size, shape, color, structure, etc.) based on the characteristics of requirement categories and risk components. These characteristics reflect the qualitative and quantitative metrics based on FCA, requirements compliance levels, and the domain semantics learned from the PDO. We discuss the developed visual metaphors based on this philosophy in the following sections.

4.6.1 Cohesive Bar Graph Visual Metaphor. A formal concept generates cohesion among requirement categories in its extent by establishing their necessity and sufficiency to understand the potential for risk due the combinations of risk components in its *intent*. We visualize this characteristic of the requirement categories in the extent a formal concept using the "cohesive bar graph" visual metaphor as shown in Figure 7. Each bar in the metaphor corresponds to a requirement category in the example scenario.

Visual features of a bar are computed as follows.

— *Color*. To understand the potential for risk due to the risk components in the *intent* of the formal concept, a colored bar indicates that the corresponding requirement category is "necessary" to be evaluated; whereas a black bar is not. The set of all colored bars indicates the set of requirements which are "sufficient" to understand the potential for risk due to the risk components in the intent of the formal concept. The color of a bar corresponds to the compliance level of the corresponding requirement category. Green represents compliance; Yellow represents partial compliance; Red represents noncompliance; and White indicates absence of evidence. The color is determined based on the lowest compliance level among requirements that the

requirement category abstracts in the analysis pool. This decision is driven by the fact that security is as good as the weakest constraint.
— *Height*. It is relative to the requirement category correlation index (Section 4.5).
— *Width*. It is relative to the ratio of the number of risk components related to a requirement category, and the total number of risk components in the formal context. Larger the width of a bar for a requirement category, larger is its relative coverage of risk components in the given scenario.
— *Ordering*. It is based on height and then width (for bars with the same height).

To maintain a consistent structural view of the metaphors across all formal concepts, presence/absence of requirement categories in the extent is indicated using colors rather than structural changes. In addition, the attributes chosen for ordering the bars is independent of the formal concept. The explanation of a formal concept (Section 4.4.4) provides additional context to the visual metaphor.

4.6.2 Cohesive Arc Graph Visual Metaphor. The cohesive bar graph can be complemented by a metaphor that visualizes the degree of influence that each requirement category has on the effective implementation of other requirement categories in a given scenario. The cohesive arc graph metaphor (inspired by Schedl et al. [2005]) visualizes this characteristic for each requirement category in the formal context. This metaphor for two requirement categories in the example scenario is shown in Figure 8. The requirement category of interest is first represented as a circle, with a color that represents its compliance level. Then, each equally angled arc around the circle corresponds to a requirement category in the formal context other than the one in the middle. Visual features of an arc are computed as follows.

— *Color*. It represents the compliance level of the requirement category as discussed for the cohesive bar graph.
— *Radius and Ordering*. The arc radius and ordering corresponds to the Requirement Influence Factor (RIF) metric. Based on the similarity coefficient, RIF is a ratio of the number of formal concepts shared between the requirement category in the middle and the requirement category represented by the arc, and the number of formal concepts in their union. The higher the RIF, higher is the similarity of the two requirement categories in correlating with other categories in the given scenario.

The cohesive arc graph visual metaphor lacks any angular modulation of the arcs to avoid many pitfalls commonly associated with pie chart visualizations [Good and Hardin 2006]. The cohesive arc graph modulates the length of equally angled arcs, in contrast to pie charts which modulate the angle of equal length arcs. The resulting visualization is essentially equivalent to wrapping a sorted bar graph on a circle. This presentation permits intuitive graphical perception based on difference in length of the arcs (and not angle as in traditional pie charts) [Cleveland 1985]. The primary motivation for a circular arrangement is to make the selected requirement a visual focal point when considering its similarities with other categories in the given scenario.

As a derived visual metric, the total fill area of the arcs allows comparing requirement categories based on their ability to strengthen the level of compliance with other requirements in the given scenario. Drawn roughly to scale, Figure 8 allows such comparison between the R5: Monitoring and the R4: Network/Internet Access Control requirement categories.

4.6.3 Noncompliance Impact Analysis. The visual metaphors combined with the concept lattice allow visualizing the propagative impact of noncompliance and corresponding potential for risk. Adopting the techniques in Tonella [2003], such analysis can be

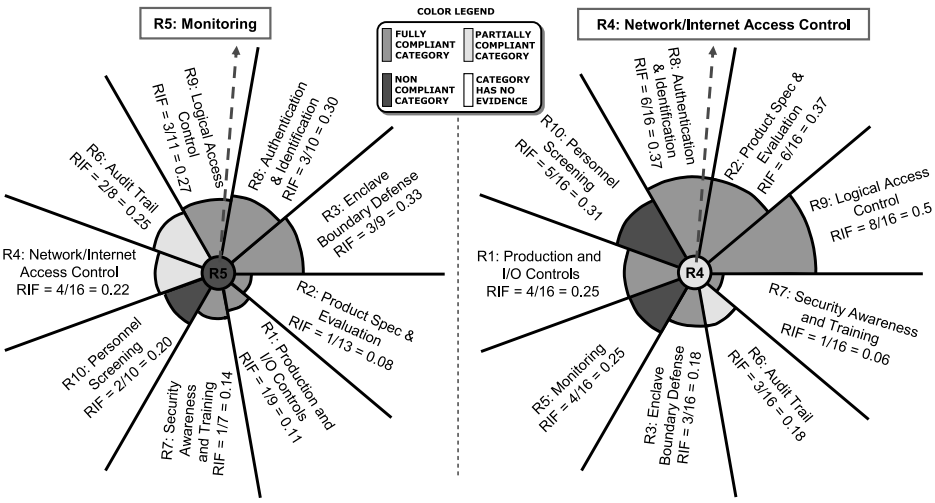

Fig. 8. Cohesive arc graph visual metaphors.

visually conducted based on a two-step procedure: (1) Localization of noncompliant nodes: Localize the formal concepts that are directly affected by noncompliance. Essentially, we identify the formal concepts that are uniquely associated with the noncompliant requirement categories (Equation (7)); and then (2) Propagation of noncompliance: For the formal concepts identified in the previous step, investigate all the formal concepts that are reachable via ascending paths in the concept lattice to reason about the propagative effects of noncompliance on other requirement categories in the scenario. During upward traversal, the visual metaphors in the context of each formal concept promote a gradual learning and discovery of such propagative effect. Figure 9 visualizes the noncompliance impact analysis for the R5: Monitoring requirement category of the example scenario.

During upward traversal in the lattice, as shown in Figure 9, requirement categories in the extent of each encountered formal concept are examined for their compliance levels and their potential to correlate with each other such that the noncompliance in one of the categories can influence the effectiveness of the security constraints imposed by the other. To facilitate this process, visual metaphors reduce the cognitive burden by readily illustrating the compliance levels as well as metrics computed from the methodology. This information would otherwise require tedious inspection and computation using the concept lattice. Visual metaphors permit abstractions of the available computational models to focus more attention on understanding the potential for risk in a given scenario.

4.7 Summary of the Methodological Steps

The evolution/improvement in "understanding the potential for risk" can be observed in progression through the steps of our methodology. In the initial phase, risk is understood in the context of an individual requirement. An investigator gains an in-depth understanding of the risk components explicated from each regulatory security requirement considered applicable in the selected operational scenario. Building upon this foundation, the following phase of the methodology provides an understanding of the potential risk due to cascading effect of failure among the diverse security requirements that work collectively to assure secure software system behavior during operation. This phase helps to organize and structure the interdependencies among

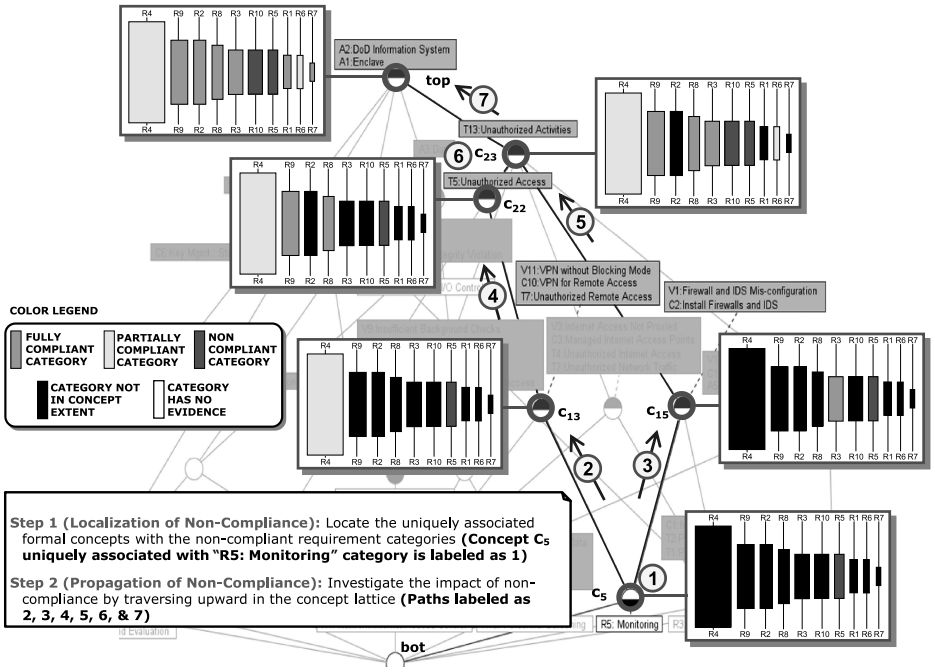

Fig. 9. Noncompliance impact analysis.

requirements based on the computational models afforded by FCA and domain semantics captured in the PDO. The third and final phase combines the characteristics of requirements and risk components discovered in the previous phases along with requirements compliance levels to produce metaphors that visually reveal the nature of possible risks. The visual metaphors are geared towards promoting human intuition in a complex and multidimensional problem space. A chain of evidence maintained through all three phases is crucial to the effectiveness of the methodology and produce meaningful insights for understanding the potential for risk based on the level of compliance with C&A requirements.

5. METHODOLOGY EVALUATION

The purpose of the methodology outlined here is to provide analytical capabilities to Subject Matter Experts (SMEs) through the execution of its steps. Planning the systematic capture and measurement of these capabilities, as methodology outcomes, is important for outlining an initial evaluation strategy that can be sustained over a period of time, in different contexts and in different domains. We define an outcome as a statement that describes what a SME is expected to know and to be able to perform by using the methodology or the expected quality of resulting artifacts. In this preliminary stage, our attempt is to systematically identify the aspects of the methodology that make the most sense to be investigated with respect to the desired outcomes. With these aspects identified, we have gone a step further to elicit qualitative feedback from a focus group of C&A practitioners and other security experts at large, during methodology application and execution for a problem scenario. We use this feedback as preliminary evidence for examining the applicability and feasibility of the presented methodology in current practice. The initial feedback has also indicated areas where the methodology can potentially be improved upon. In the following section we discuss

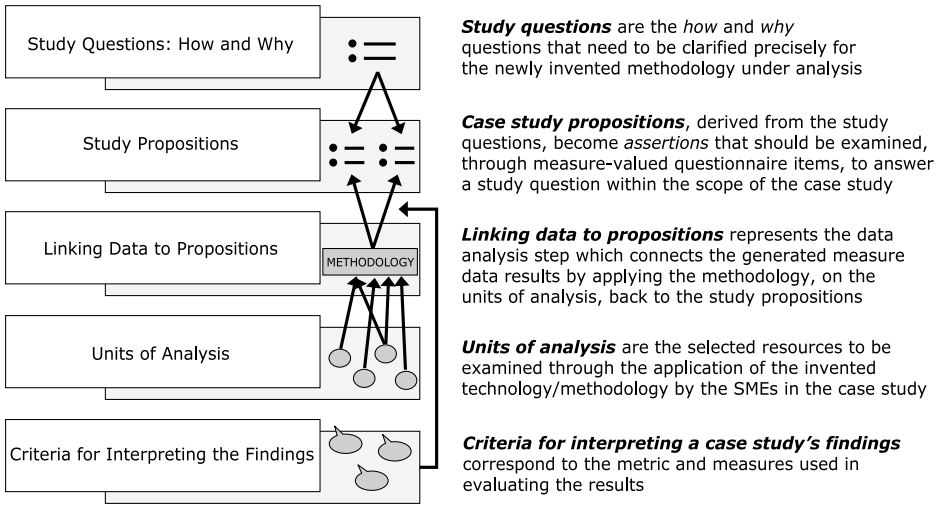

Fig. 10. Components of case study research design [Lee and Rine 2004].

our efforts to first identify what characteristics of the methodology are relevant to its evaluation.

5.1 Case Study Research Design

In context with experts, an investigator can be tempted to collect a lot of data (metrics and measures) during methodology execution to examine the achievement of desired outcomes. In this circumstance, it is first necessary to rigorously plan the followings: the characteristics of the methodology to study; what data are relevant; what data to collect; and how to analyze the results [Lee and Rine 2004; Yin 1994]. To systematically conduct this planning exercise, we have selected the case study research design methodology. Lee and Rine [2004] made one of the earliest contributions towards a systematic goal-oriented case study research design for software engineering methodology validation. In this section we discuss the instantiations of case study research design components, as shown in Figure 10.

A study question clarifies the purpose of the investigation while emphasizing its explanatory nature [Yin 1994]. We investigate the following question: *How* and *why* does the execution of the methodology improve the understanding of the potential for risk during system operation, given the compliance evidence from certification activities?

Propositions as claims refine the study question to direct attention towards the characteristics of the methodology that should be investigated. Based on our theories, the propositions are: 1) The methodology execution improves the ability to select a scope and justify the criteria adopted for understanding the potential for risk during system operation; 2) The potential for risk due to cascading effect of failure among security constraints imposed by regulatory security requirements is discovered and understood in the context of system operation; 3) The metrics and measures from the methodology improve the ability to later conduct a comprehensive cost-benefit analysis with respect to the level of compliance required with regulatory requirements; and 4) The artifacts from the methodology improve the ability to analyze and communicate the potential for risk during system operation due to noncompliance with C&A requirements.

To evaluate the propositions, the units of analysis to be examined by SMEs include the followings: the steps in the methodology; the artifacts used or resulting from the steps; and the analytical activities performed upon the artifacts. To make meaningful

Table IV. Summary Sheet

QUESTIONNAIRE SET 1 STEP 1: GOAL-DRIVEN SCENARIO COMPOSITION	QUESTIONNAIRE SET 2 STEP 2: ANALYSIS POOL FORMATION	QUESTIONNAIRE SET 3 STEP 3: ABSTRACTIONS IN THE ANALYSIS POOL
1.1 Does Goal-driven Scenario Composition (GDSC) systematically scope analysis?	**2.1** Does analysis pool formation help to justify search criteria and collect applicable regulatory requirements for understanding the potential for risk during system operation?	**3.1** Do abstractions in the analysis pool help focus on different classes of security constraints?
1.2.1 Rate the perceived ease of goal identification	**2.2** Rate the following search strategies **2.2.1** Keywords from goals and scenario **2.2.2** Keywords from domain expertise **2.2.3** Related keywords from documents **2.2.4** Focused Hierarchical Browsing **2.2.5** Multi-dimensional Browsing **2.2.6** Hierarchical Browsing	**3.2** To what extent are abstractions in the analysis pool helpful to reduce and effectively manage its complexity?
1.2.2 Rate the perceived ease of scenario identification	**2.3** Rate the perceived assurance of identifying an exhaustive collection of applicable requirements based on multiple search strategies	**3.3** To what extent are abstractions in the analysis pool helpful to focus on the collective effectiveness of security constraints?
1.3 What sources other than operational scenarios are valuable to trigger risk assessment?	**2.4** Does the problem domain ontology help to contract/expand the search space of requirements?	
1.4 How does GDSC differ from current practices?	**2.5** Does gathering compliance evidences in the context of the analysis pool improve the understanding of the potential for risk due to non-compliance?	
1.5 Does a multi-dimensional explication of regulatory requirements improves their understanding	**2.6** Does the quality of the RTM improve by explicit association of operational scenarios with regulatory requirements and their compliance evidences?	
1.6 Are the dimensions in the problem domain ontology sufficient in a socio-technical environment?	**2.7** Rate overall effectiveness of GDSC in coupling the risk assessment process with understanding regulatory requirements and their applicability	
1.7 Do the concepts associated with regulatory requirements in the problem domain ontology provide a baseline to understand and identify risks in a given organizational environment?		

QUESTIONNAIRE SET 4 STEP 4: CREATING A MODEL OF CORRELATIONS	QUESTIONNAIRE SET 5 STEP 5: RISK METRICS AND MEASURES	QUESTIONNAIRE SET 6 STEP 6: ENABLING INSIGHTS
4.1 Does the Formal Context help visually perceive patterns of significant interaction among security constraints based on various risk components?	**5.1** Rate the perceived usefulness of the risk upper and lower bound metrics for later conducting a cost-benefit analysis to minimize risk	**6.1** Rate the perceived usefulness of non-compliance impact analysis in understanding the risks due to propagative effects of non-compliance
4.2 Does augmenting the Formal Context help identify security constraints specified at different levels of abstraction in regulatory requirements?	**5.2** Rate the perceived usefulness of the requirements correlation metric in prioritizing regulatory requirement categories for later conducting a cost-benefit analysis to minimize risk	**6.2** Rate the cohesive bar graph visual metaphor for its ability to improve the understanding of a formal concept and the metrics associated with it
4.3 How are regulatory requirements specified at different levels of abstraction currently considered and evaluated?	**5.3** Rate the perceived usefulness of the requirements correlation metric and requirements compliance levels to convey the propagative effects of non-compliance	**6.3** Rate the cohesive arc graph visual metaphor for its ability to improve the understanding of the influence of requirement categories on each other
4.4 Does augmenting the Formal Context help identify risk components specified at different levels of abstraction in regulatory requirements?	**5.4** Rate the perceived usefulness of the risk criticality metric in prioritizing risk components for later conducting a cost-benefit analysis to minimize risk	**6.4** Rate the perceived usefulness of the requirement influence metric to understand the criticality of a requirement category for strengthening the level of compliance with a large proportion of requirements
4.5 Does augmenting the Formal Context improve the identification of the extent of potential risks?	**5.5** Rate the perceived usefulness of the risk criticality metric and requirements compliance levels to convey the propagative effects of non-compliance	**6.5** Rate the ability of cohesive bar graph and cohesive arc graph for their ability to improve non-compliance impact analysis and convey its results
4.6 Rate the visual intuitiveness of the Concept Lattice to understand correlations among regulatory requirements based on related risk components	**5.6** Do implication rules help to understand the patterns of significant interactions among risk components?	**6.6** Rate the overall effectiveness of Formal Concept Analysis (FCA) and the resulting metrics in reasoning about potential risks
4.7 Rate the usefulness of visualizing different classes of risk components based on the Concept Lattice	**5.7** Rate the effectiveness of implication rules to convey risk coverage due to non-compliance	**6.7** Rate the overall effectiveness of FCA and the resulting metrics in improving the documentation and communication of risk
4.8 Rate the usefulness of Formal Concepts to understand "necessity and sufficiency" of regulatory requirements in understanding risks?		**6.8** Rate the overall effectiveness of visual artifacts to improve the analytical capabilities to reason about risk
4.9 Rate the usefulness of Explanations in interpreting Formal Concepts for understanding the potential for risk due to non-compliance?		

observations while examining these units of analysis, a "Summary Sheet" is prepared for use by SMEs. The summary sheet is a collection of questionnaires that correspond to each step in the methodology. Propositions influence the design of each question by including specific propositions as metric criteria to examine the units of analysis. Combined with given instructions, the summary sheet guides SMEs to make observations during the methodology execution without interventions from the investigator, while making the process repeatable. Table IV is a concise presentation of the summary sheet.

5.2 Expert Selection

For a preliminary investigation, our case study research design was used in the context of DITSCAP [DoD 5200.40 1997] to elicit qualitative feedback from SMEs. However,

the defense domain and the sensitive nature of C&A documentation for critical systems put several limitations on our study. C&A being a highly specialized field; it is difficult to find experts for DITSCAP. Their limited availability and high cost also restrict the study duration. Sensitivity of organizational knowledge in the defense sector further discourages the availability of ongoing C&A efforts or participation of experts in experimental studies. Fortunately, under agreement of nondisclosure of their identities, SMEs with extensive experience (10+ years) in various types of C&A processes, including DITSCAP, volunteered to participate in our case study. To gain insight from diverse viewpoints, SME selection for the first study included one from a government/defense organization (referred as SME_{gov}) and another from a privately owned firm (referred as SME_{pri}).

To expand the scope of our results, the first study was followed by two additional studies. These studies involved SMEs with general security and risk assessment experience including C&A. The second study was performed with a Project Team Leader/Branch Chief at a defense agency with significant experience (10+ projects, 10+ years) in enterprise-wide network risk assessment (referred as SME_{era}). The third study involved a Technical Writer (referred as SME_{tec}) for a major defense contractor with documentation experience on enterprise-wide security and C&A projects including DITSCAP. In all three studies with four SMEs, a purposeful SME selection ensured coverage of a diverse range of experience with C&A, system security and risk assessment activities in different roles.

During our investigation, SMEs as participants observed the step-wise methodology execution in the context of a hypothetical software system and its operational scenario, which have been used as an example throughout this article. These observations were followed by an open-ended question/answer session with the investigators. After these given instructions, without interventions from the investigators, SMEs filled out the summary sheet, while the steps in the methodology execution and its artifacts were available for quick reference as tutorial notes. Finally, the SMEs engaged in an open discussion to provide additional insights towards their responses.

5.3 Linking Data to the Propositions and Criteria for Interpreting the Findings

Case study research design requires an explicit logic linking the data to the propositions. Therefore, to bridge the gap between the abstract propositions and the questions in the summary sheet, we further refine the propositions into specific study claims. This refinement continues until the claims are directly relevant to the metric criteria addressed in summary sheet questions; that is, can be easily interpreted in operational terms of the methodology. Table V lists the claims identified by this heuristic.

Using the summary sheet, SMEs examine the units of analysis to express the level of confidence in the corresponding study claims as well as provide comments to further elaborate or justify their observations. To understand such qualitative data gathered from different SMEs, its intuitive presentation and structure is important. Therefore, we perform a stratification of the summary sheet responses based on the examined units of analysis and the related study claims. The resulting presentation, as shown in Table VI, allows the use of "patterns" (trends in responses) as criteria for evaluating the results.

5.4 Results and Discussion

5.4.1 Trends Across the Units of Analysis. A box plot of the row-wise average responses for each SME in Table VI across all study claims related to a unit of analysis reveals the trends (i.e., variances) in the aggregate level of confidence expressed by SMEs in the set of study claims related to each unit of analysis. For simplicity, all responses

Table V. Study Claims Derived from Propositions

Propositions	Study Claims
Propositions 1	**(C1) Trigger and Scope:** The effort to understand the potential for risk during system operation is systematically triggered and explicitly scoped
	(**C2) Requirements and Risk:** The regulatory security requirements, risk components and the relationships among them are interpreted based on a common understanding
	(C3) Justifiable Search Criteria: The criteria used to search for regulatory security requirements that help to understand the potential for risk in the system operational context is justifiable
	(C4) Exhaustive Coverage: An exhaustive collection of applicable regulatory security requirements are identified in a given system operational context
Proposition 2	**(C5) Complexity Managed:** The complexity of the problem space is effectively managed based on available abstractions for the regulatory security requirements
	(C6) Abstractions Considered: Regulatory security requirements and risk components specified at different levels of abstraction and their interdependencies are considered to understand the potential for risk
	(C7) Collective Effectiveness: The potential for risk is determined based on the collective effectiveness of diverse security constraints imposed by regulatory security requirements
Proposition 3	**(C8) Propagative Impact:** The available metrics for understanding the propagative impact of non compliance improve the ability to later conduct a cost benefit analysis
	(C9) Prioritization: The available metrics to prioritize regulatory security requirements and related risk components improve the ability to later conduct a cost benefit analysis
Proposition 4	**(C10) Analytical Capacity:** The available artifacts are intuitive for discovering and understanding the potential for risk in the system operational context
	(C11) Risk Communicability: The available artifacts improve the ability to communicate the potential for risk in the system operational context due to non

are mapped to a 5 point scale, with 5 being the highest and 1 being the lowest level of confidence expressed by the SMEs. The computed box plot is shown in Figure 11.

In Figure 11 a positive trend of consistent agreement between the SMEs is visible across a majority of the units of analysis with a median level of confidence of about 4 or higher in supporting the corresponding study claims. Any diversion from this trend requires further analysis. Based on this heuristic, a pattern of relatively low confidence can be observed for the risk metrics and measures (G) unit of analysis. SME_{gov} emphasized that the metrics "help to understand what else is affected"; however, they are "not enough" for cost-benefit analysis. SME_{pri} expressed the need for "specific details about mitigation strategies associated with the risk components or requirement categories considered in the scenario, their associated costs and other factors in the context of the software system." However, the availability of this information was beyond the scope of our hypothetical scenario. Nevertheless, both SMEs perceived that risk metrics would facilitate the usage and intuitive presentation of such quantitative information for later conducting a risk assessment. In the second study, SME_{era} perceived the risk criticality metric as an "excellent source for deciding what to tackle first", From the third study, SME_{tec} deemed the metrics to be "useful in making multiple changes (compliance related); i.e. what do I really hurt as far as risk goes" and "help justify actions and expenditures."

For the visual artifacts (H) unit of analysis, a similar trend of relatively low confidence can be observed in Figure 11. During noncompliance impact analysis, SME_{pri} observed that "going too high up in the chain (upward traversal in the concept lattice) diminishes the credibility of the overall picture." The SME further suggested that by

Table VI. Stratification of SME Responses

Units of Analysis \ Leaf-Node Claims		Trigger and Scope	Req. and Risk Understanding	Selection Criteria	Exhaustive Coverage	Complexity Managed	Abstractions Considered	Collective Effectiveness	Propagative Impact	Prioritization	Analytical Capacity	Risk Communicability
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C&A Goals and Operational Scenarios	A	1.1 D		2.7 R	2.2.1 R	1.1 D						2.6 R
		1.2.1 R			2.2.2 R							
		1.2.2 R			2.2.3 R							
		1.3 S										
		1.4 S										
Representation of Requirements in the Ontology	B		1.5 D	2.7 R	2.2.4 R						2.4 D	
			1.6 D		2.2.5 R							
			1.7 D		2.2.6 R							
					2.3 R							
					2.4 D							
Analysis Pool	C			2.1 D		3.2 R		3.1 D			2.5 D	
				2.7 R		3.3 R		3.3 R			3.3 R	
Formal Context	D						4.2 D	4.1 D			4.1 D	6.7 R
							4.3 S				4.5 D	
							4.4 D				6.6 R	
							4.5 D					
Concept Lattice	E						4.7 R	4.6 R			4.6 R	6.7 R
								4.8 R			4.7 R	
											4.8 R	
											6.6 R	
Formal Concept Explanations	F										4.9 R	6.7 R
											6.6 R	
Risk Metrics and Measures	G								5.1 R	5.2 R	5.1 R	5.3 R
										5.3 R	5.2 R	5.5 R
										5.4 R	6.6 R	6.7 R
										5.5 R		
Visual Artifacts	H								6.1 R	6.2 R	6.2 R	6.5 R
									6.2 R		6.3 R	
									6.4 R		6.8 R	
Implication Rules	I								5.6 D		6.6 R	5.7 R
												6.7 R

Legend: **Cross table Entry:** <Question number> <Question Type> <SMEpri> <SMEgov><SMEera><SMEtec>
Question Types: **(R)** Scaled Response Question, **(D)** Dichotomous Question, **(S)** Short Answer Question
Response Colors: **(R)** Scaled Responses → **5** **4** **3** **2** **1** ("**5**" being the highest and "**1**" being the lowest rating)
(D) Dichotomous Response → **Yes** **No**
(S) Short Answer Response → **Good** **Average** **Poor**

navigating to the top of the lattice, it may seem that full-compliance always becomes necessary. Rather, the original purpose of upward navigation was to systematically reason about possible propagative effect of non-compliance through gradual discovery. It is up to the analyst to identify a reasonable stopping criterion, while the lattice acts as a cognitive aid. Despite lower ratings, SME_{pri} suggested that the "cohesive bar graph is great!" and "anything helping to understand "what-if" scenarios helps obtain funding commitment/support to implement the mitigation plans." In the following studies, SME_{era} greatly appreciated the cohesive bar graph and cohesive arc graph for their ability to "immediately identify what matters and what doesn't, degree of compliance, and potential for impact on other requirements." SME_{tec} perceived an initial "learning curve," but added that "once you understand the visuals, the amount of information that can be captured and understood is far greater than through other means." In addition, SME_{tec} expressed that "the visuals will help the risk managers and nontechnical managers quickly grasp technical/complex issues they don't understand or have time for."

5.4.2 Trends Across the Study Claims. A box plot of the columnwise average responses for each SME in Table VI across all units of analysis related to a study claim reveals the trends (i.e., variances) in the aggregate level of confidence expressed by SMEs in

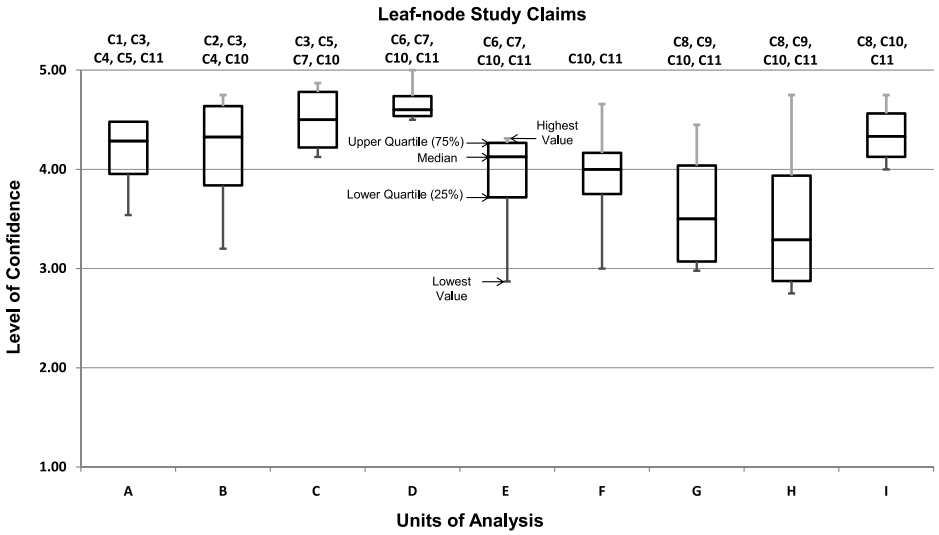

Fig. 11. Trends in the confidence levels of SMEs across the units of analysis.

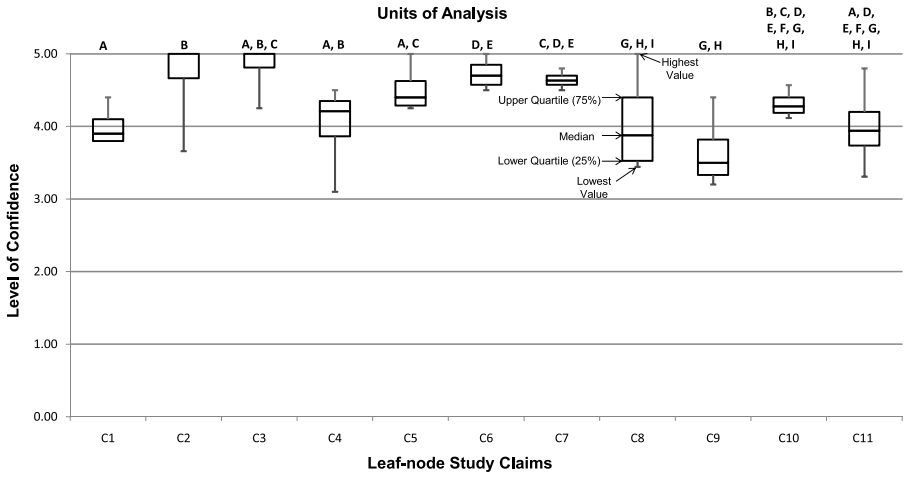

Fig. 12. Trends in the confidence levels of SMEs across the leaf-node study claims.

the set of all units of analysis related to each study claim. The resulting box plot is shown in Figure 12.

The box plot in Figure 12 can be intuitively examined based on groups of study claims refined from the same high level proposition. For example, the graph demonstrates a trend of high confidence for all study claims (C5, C6, and C7) related to *Proposition 2*.

Within the group of claims refined from Proposition 1, slightly lower confidence is observed for the study claim "C1". SME_{gov} praised the process of goal-driven scenario composition to trigger risk assessment as being analogous to "biting of small chunks to eat the elephant"; however, raised concerns that in practice the certifiers may have little or no strategic knowledge to identify appropriate goals and scenarios. We argue that the notion of "scenario" is quite broad and they can be easily identified from a

variety of nonconfidential sources. Other SMEs also emphasized the systematic nature of the goal-driven scenario composition to trigger and scope the analysis effort.

For Proposition 1, claim "C2," SME_{gov} differed significantly from others; however the associated explanation provides more useful insight. SME_{gov} suggested that regulatory requirements "warn [against risks] as a general rule, but not a specific rule. They state a good place to start, but are likely in need for tailoring." In the private sector the focus is on "expending just enough resources to achieve compliance with regulatory requirements and get approval to operate"; whereas in the government sector "the regulatory requirements are perceived as a minimal baseline that is further built upon to protect critical national interests." These arguments corroborate with the strong confidence expressed by all SMEs for analysis pool formation in Step 2 of the methodology, related to claim "C3," which grounds the abstract understanding of regulatory requirements in the context of operational system scenarios. SME_{pri} observed that "... these steps will help build "real" risk assessment results rather than "carved" answers to meet regulatory requirements." SME_{era} emphasized that "goals and scenarios make C&A more real $\rightarrow$ ties to realistic operations and potential impact."

Finally for Proposition 1, claim "C4," the SMEs differed on the perceived usefulness and their preference for the different search techniques. While SME_{pri}, SME_{era}, and SME_{tec} demonstrated high confidence in both keyword and exploration based search techniques, SME_{gov} was only inclined towards the use of keyword-based techniques. These differences suggest idiosyncratic search habits as well as preference for simpler and familiar search techniques.

The variations in the levels of confidence of SMEs with respect to claims "C8" and "C9" derived from Proposition 3, to a large extent result from the responses elicited in context of the units of analysis G and H (This is clearly visible in Table VI). These aspects have been discussed extensively in Section 5.4.1.

The claims "C10" and "C11," derived from Proposition 4, aggregate responses from several units of analysis throughout the methodology. A closer look reveals that all SMEs expressed a high and consistent confidence in the "intuitiveness" of the artifacts from the methodology for risk assessment (claim "C10"); however, their average responses varied significantly on the "communicability" of the artifacts (claim "C11"). SME_{gov} expressed that "the communication [of the artifacts] is good but the documentation should follow a more organizationally relevant format." In contrast, SME_{pri} suggested that the artifacts help to "show the due diligence behind the analysis," and SME_{era} expressed that the metrics from FCA "provide analytical rigor" for the documentation and communication of risks due to noncompliance. Different SME background may have contributed to the observed variance in responses. For example, strict controls exist in the government and defense sector to adhere to defined documentation guidelines, whereas in the private sector intuitive and compact reports are given more importance (e.g., dashboards). C10 and C11 being general claims about the characteristics of methodology as a whole, are examined in the context of multiple units of analysis spanning several steps of the methodology. A mix of general and specific claims facilitates evidence collection at different levels of granularity with respect to the propositions.

5.4.3 Supplemental Observations. Despite limited or no prior experience of the SMEs with ontologies, the PDO was perceived as a huge improvement over natural language documents. It is also noteworthy that with our limited domain expertise; the set of requirements discovered to be applicable in our hypothetical scenario were acceptable to SMEs with 10+ years of experience across a variety of C&A and risk assessment projects. The requirements were identified by solely relying on the requirements representation in the PDO and the steps in our methodology. This observation promotes

confidence in the use of ontologies for regulatory requirements modeling and analysis during C&A activities.

The SMEs demonstrated no difficulty in understanding FCA and they learned to interpret the concept lattice with minimal instructions. The SMEs used the concept lattice to discuss potential overlaps among regulatory requirements, which they were not able to observe or clearly express before. SME_{pri} expressed that: "being able to look at the concentration/areas of significant overlap [among requirement categories] is invaluable." While examining formal concepts and their explanations, SME_{gov} emphasized that they help to "take out the ambiguity" in conducting risk assessments. SME_{tec} identified the "lattice to provide a multidimensional look that has not been available before." SME_{era} found the explanations to be highly intuitive in spelling out "the source of risk and the level of compliance in a specific scenario."

In summary, the qualitative feedback from C&A practitioners and security experts provide preliminary evidence for the merit of our methodology towards understanding the potential for risk due to regulatory noncompliance in an operational scenario. This study has also identified several areas of the methodology that require refinement/improvement as well as the aspects that require further exploration in well-designed case studies involving complex, task-based settings of an ongoing C&A project; for example, an in-depth investigation of the use of visual metaphors and their impact on the perception of the possibility of harm or loss.

5.5 Threats to Validity

Although the nature of the current investigation is qualitative in nature, a discussion of the case study design based on various logical tests promotes further insights into the value of our results.

— *Construct Validity*. A chain of case study evidence exists through the decomposition of the study question into propositions; and the propositions into study claims (Table V), which are then finally associated with summary sheet questions (Table VI) presented during methodology execution. This traceability promotes confidence in the selection of the right measures in the summary sheet for the characteristics of the methodology being studied. The use of specific propositions as metric criteria in the design of each summary sheet question prevents "subjective" judgments in planning data collection. Finally, SMEs with extensive experience in performing C&A and risk assessment, as our sources of evidence, further confirm the appropriateness of the measures selected to suggest methodology benefits for understanding the potential for risk due to noncompliance.
— *Internal Validity*. In contrast to spurious causal relationships between the method and result, the methodology presented here outlines a rich theoretical background along with step-by-step guidance for SMEs to produce certain predefined models/artifacts. These incremental steps and the resulting artifacts maintain a causal chain of evidence for the characteristics of the methodology being investigated. In addition, an explicit explanation for the existence of each artifact is available through the models and techniques used in the steps of the methodology.
— *External Validity*. In practice, the DITSCAP and its regulatory requirements are generally considered to provide more specific and detailed technical guidance as compared to other C&A processes. For example, DITSCAP requirements have been used in practice to guide the implementation of security controls required for HIPAA [Mitchell 2005]. In terms of applicability to a broader set of secure software engineering practices outside of the C&A domain, the DITSCAP regulations heavily cross-reference the best practices originating in widely used standards of the National Institute of Standards and Technology (NIST). These characteristics of the

DITSCAP regulatory requirements to some extent may have facilitated the process of constructing the PDO. However, despite the extensive coverage of security issues by DITSCAP regulatory requirements, the understanding and perception of risk to information systems resulting from the C&A process is still poor and questionable [US GAO 04-376 2004; US GAO 05-700 2005; US GAO 07-837 2007]. Our methodology is geared towards addressing the gap between the evidence for compliance with regulatory requirements and its interpretation in terms of the operational risk. We believe that identifying the potential for risk due to noncompliance with regulatory requirements in the context of a large and complex system requires a systematic approach to understanding and discovering the correlations between regulatory requirements.

Completeness of the DITSCAP requirements cannot be proven, but they should be seen as a necessary and sufficient set of requirements derived based on the threat model perceived by the DoD. Furthermore, the DIACAP standard [DoD 8510.01 2007] that now supersedes DITSCAP to enable dynamic collaborations for C&A within a net-centric infrastructure makes little or no changes to the list of regulatory requirements. Such comprehensiveness and wide outlook of the DITSCAP requirements significantly boosts the possibility of replicating our results in domains other than C&A. In addition, our methodology relies on a requirements and risk model (Figure 2) that is extended from the Common Criteria [2006] security model, and requirements engineering best practices.

— *Reliability*. Our thorough research design provides a repeatable protocol for case study execution and data analysis. A step-wise methodology execution with predefined artifacts, a documented problem scenario, and the summary sheet have been used to ensure repeatability of the data collection procedure during our preliminary investigations with four SMEs in a total of three meetings. Finally, subjectiveness in the opinion of an expert is addressed by involving multiple SMEs in our study with different organizational backgrounds, experience and technical expertise with respect to C&A and risk assessment.

6. RELATED WORK

Identifying, analyzing, assessing and managing risk is an integral part of designing practical and cost-effective secure systems [Alberts and Dorofee 2001b; Baskerville 1993; Geer 2003; McGraw 2006; Schneier 2000; Stoneburner et al. 2002]. Essential precursor to an effective risk assessment is a process of understanding the potential for risk during system operation by analyzing the interdependencies among various system defenses and their relation to the risk components of threats, assets and vulnerabilities. With growing system complexity and numerous multifaceted security requirements at different levels of system details, this process is rarely conducted systematically. In this paper we have outlined a regulatory requirements-driven approach to identify and understand the potential for risk in system operational scenarios and then systematically reason about the possible outcomes due to noncompliance or varying degrees of compliance.

To assure requirements satisfaction by a "machine," one needs to understand the nexus of constraints and causal chains in the problem domain [Jackson 1995]. For security requirements, such reasoning are naturally driven by threat analysis (i.e., agent, motive, means, and opportunity) based on the fundamental abstractions of Goal, Scenarios and Viewpoints used heavily in requirements engineering research. Scenario-based methods perform such analysis by identifying misuse cases [Sindre and Opdahl 2000], abuse cases [McDermott 2001], abuse frames [Lin et al. 2004] (based on problem frames [Jackson 1995]), and issues/failures/hazards in functional requirements [Donzelli and Basili 2006]. In contrast, goal-based methods use intentions to identify

potential threats, which include modeling of social relationships among actors/agents as soft goals to be satisfied [Lin et al. 2003], attack trees [Schneier 2000], intruder anti-goal modeling [van Lamsweerde 2004], and modeling risk as an event that prevents goal satisfaction [Yudistira et al. 2006]. Modeling interactions between functional and security goals has been suggested [Moffett et al. 2004] to identify threats to assets. The Goal Question Metric (GQM) [Basili et al. 1994] philosophy is also fundamental to approaches for evaluating security constraints throughout the organization [Chew et al. 2008; Johansson and Johnson 2005; Vaughn et al. 2002]. Viewpoint-based methods advocate the identification of stakeholders with security viewpoints [Kotonya and Sommerville 1996] to include security concerns in various engineering decisions. Viewpoints are fundamentally useful for identifying conflicting requirements [Easterbrook 1993], which may identify the possibility for a security risk. From this discussion, it is apparent a single requirements method is clearly insufficient to model regulatory security requirements. Therefore, in building the PDO we leverage the strengths of multiple requirements engineering philosophies to explicate regulatory security requirements from multiple dimensions relevant to proactively reveal the potential for risk due to their interdependencies in the context of system operational scenarios. Existing approaches rely heavily on domain experts first to elicit and model interactions among system features [McDermott 2001] and then identify the potential for risk.

Capturing domain concepts and their interdependencies in the universe of discourse is fundamental to many research initiatives to understand nonfunctional requirements. Cysneiros et al. [2004] use a hyperlinked lexicon of domain concepts to integrate nonfunctional and functional requirements. To formalize natural language descriptions of the system and environment in nonfunctional requirements, Breaux et al. [2009] use a dictionary that maps the words in a lexicon to their meanings in an ontology. [Feather and Cornford 2003] suggest the development of requirements and fault hierarchies to analyze their interdependencies. Because nonfunctional requirements span across levels of abstraction in multiple dimensions, to fully understand them, we rely on hierarchical classification and categorization of regulatory security requirements, their associated domain concepts and the interdependencies among them captured in the PDO. The PDO facilitates our analysis to be conducted simultaneously at many levels of abstraction in multiple dimensions using FCA.

Frameworks for risk assessment, such as the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE^{SM}) [Alberts and Dorofee 2001a; Alberts and Dorofee 2001b], NIST 800-30 [Stoneburner et al. 2002], CORAS [Aagedal et al. 2002] and Risk Management Framework (RMF) [Verdon and McGraw 2004], usually begin with asset enumeration, threat modeling and analysis, followed by assessing possible damage to assets due to exploitable vulnerabilities and finally producing risk mitigation plans by selecting countermeasures. Salter et al. [1998] use a mapping between attacker characteristics and vulnerabilities throughout the system life cycle, to identify the potential for risk. Quantitative risk-centric decision processes [Buckshaw et al. 2005; Butler 2002; Feather and Cornford 2003; SooHoo 2000] rely on quantifying the interactions among risk components based on expert intuition or past experiences/records. However, the accuracy of these risk estimates relies heavily on the rigor in identifying all potential risk components and their interactions within the boundary of investigation. It has been observed that precise quantification of risk is difficult to develop, costly, can be misleading and generally very specific loss estimates are not necessary to decide the implementation of a countermeasures [Pfleeger and Pfleeger 2003; Peltier]. Furthermore, despite mathematical rigor, an inaccurate description of the real-world phenomena will only produce inaccurate results. To leverage the true potential of quantitative approaches, in the face of increasing system complexity, our work provides a regulatory requirements-driven baseline for systematically

identifying and justifying the risks components and their interdependencies to be considered in a certain investigation. A bounded context further helps to manage the computation complexity associated with quantitative methods. The consideration of the system operational environment and compliance evidence from regulatory requirements may also improve stakeholder participation and the transparency of the results from quantitative risk assessment methods.

Recent efforts for improving the representation of regulatory requirements have been towards providing attributes that help to classify and categorize them. For example, to conduct certification based on regulations in the United Kingdom, the CRAMM toolkit [Siemens UK 2005] maintains a library consisting of over 3000 detailed countermeasures organized into over 70 logical groupings. The DIACAP [DoD 8510.01 2007] explicitly identifies related threats and vulnerabilities for each security requirement maintained in its electronic databases. This move towards rich, meaningful representations of regulatory requirements is essential to certify software systems that continue to grow as complex and interconnected systems of systems supporting diverse socio-technical environments.

Integrated security requirements engineering frameworks such as SQUARE [Mead et al. 2002], define risk assessment as an integral part of their methodology. However, the selection of a technique for risk assessment and its practice is left entirely up to the analyst, leading to loose integration with security requirements. In contrast, our approach is to tightly couple the evaluation of security requirements with risk assessment based on a fundamental (and first of its kind) model of their relationships, as shown in Figure 2.

7. CONTRIBUTIONS AND FUTURE WORK

This work contributes a novel approach to understand the level of compliance with regulatory requirements in terms of the potential for risk during system operation. The corresponding methodological steps facilitate the discovery and understanding of multidimensional correlations among regulatory requirements. These multidimensional correlations facilitate the exploration of cascading effects of failure in the system operational context, which are often missed due to a lack of structure in natural language requirements specifications and the complexity of such analysis. In a given scenario, the artifacts constructed from the methodology demonstrate the necessity and collective sufficiency of the security constraints imposed by regulatory requirements with respect to the related risk components using well-defined metrics and explanations. Visual analytics facilitate reasoning in a complex and multidimensional problem space by raising the level of abstraction using the available computational methods of FCA and the domain semantics from the PDO. The methodology also makes several contributions to improve documentation during the C&A process. First, the notion of risk is tightly integrated with the applicability of and compliance with regulatory requirements in the context of the software system. Second, well-defined metrics and measures facilitate an overall risk-based strategy to determine the required level of compliance with regulatory requirements. Third, visual illustrations are accessible to diverse stakeholders for understanding C&A documentation. Fourth, well-defined artifacts act as a baseline to guide the creation of task reports required for various C&A activities for later conducting an extensive risk assessment. For example, the collection of analysis pools can provide a baseline to identify the threat model of a system and vice versa. Finally, the artifacts from the methodology bridge the gap between the understanding of functional system needs and the required nonfunctional regulatory security requirements to maintain an acceptable level of risk.

Human knowledge is embedded in several aspects of the methodology execution such as the requirement specifications in regulatory documents; the classification and

categorization of domain concepts in the PDO; the selection of scenarios to trigger the methodology; the selection criteria for requirements applicability in the analysis pool; the construction of compliance instruments used to measure the level of compliance with regulatory requirements; and the most importantly the domain expertise and the analytical capabilities of the SMEs who perform the steps in the methodology. Furthermore, a regulatory requirement-driven approach to understand risk will only be as good as the requirements themselves. To evaluate our methodology, in the presence of such diverse human factors, we have presented a rigorous case study research design that led to a preliminary but effective setup to gather qualitative feedback from SMEs with experience in C&A and risk assessment fields. Analysis of the gathered feedback demonstrate a highly encouraging trend towards the applicability and feasibility of the methodology in addressing the current challenges for understanding the true potential for risk due to noncompliance.

Our findings also suggest certain shortcoming of the methodology. These characteristics include: 1) The lack of consideration of quantitative data (e.g., asset value, threat frequency, vulnerability exposure, countermeasure cost, requirement criticality, etc.) related to regulatory requirements and risk components to later conduct a precise cost-benefit analysis; 2) The possibility of over generalizing the cascading effect of failure in the absence of a stopping condition for the propagative effect of noncompliance during impact analysis using FCA; and 3) A possible learning and adoption curve for a new methodology and its artifacts.

The methodology, in its current stage, focuses on individual operational scenarios in a bounded and local system scope. However, as a large assortment of analysis pools become available, recurring structures in their *concept lattice* can detect correlations among requirements across scenario networks [Alspaugh 2002] or unrelated scenarios based on similar risk components or regulatory requirements. Such analysis may reveal the potential for security breaches due to seemingly unrelated system-wide events. Presently, we are investigating such correlations at a global system-wide scope based on structural analogical inferences [Gentner 1983] across analysis pools as well as identifying groups of analysis pools that resemble pre-defined interaction patterns among domain concepts in the PDO. In addition, during the creation of an analysis pool for a scenario, our search techniques use the ontological representation of requirements to expand the scope of the scenario to requirements and related risk factors which may be initially overlooked.

We are also currently working towards a quantitative model of risk assessment involving the concepts in the security requirements and risk components model in Figure 2. The resulting model will quantify how much each risk component, if it occurs, impacts other related risk components. Such quantitative data can be based on historical/statistical analysis or intuition from a domain expert. The quantitative risk assessment techniques will then add to the repertoire of analysis methods available in an integrated framework to understand and analyze the potential for risk based on regulatory requirements. Our ongoing work also focuses on improving the usability of the integrated requirements-driven C&A workbench [Lee et al. 2007b] that supports the methodology presented in this paper.

REFERENCES

AAGEDAL, J. O., DEN BRABER, F., DIMITRAKOS, T., GRAN, B. A., RAPTIS, D., AND STOLEN, K. 2002. Model-based risk assessment to improve enterprise security. In *Proceedings of the 6th International Enterprise Distributed Object Computing Conference*. 51–62.

ALBERTS, C. AND DOROFEE, A. 2001a. OCTAVE Criteria v2.0. Software Engineering Institute, Carnegie Mellon University.

ALBERTS, C. AND DOROFEE, A. 2001b. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE^{SM}) Method Implementation Guide, v2.0. Software Engineering Institute, Carnegie Mellon University. http://www.cert.org/octave/octavemethod.html.

ALEXANDER, I. 2003. Misuse cases: Use cases with hostile intent. *IEEE Softw. 20*, 1, 58–66.

ALSPAUGH, T. A. 2002. Scenario networks and formalization for scenario management. Ph.D. thesis, North Carolina State University.

ARMSTRONG, W. W., NAKAMURA, Y., AND RUDNICKI, P. 2002. Armstrong's axioms. *J. Formaliz. Math. 14*.

BAADER, F., CALVANESE, D., MCGUINESS, D., NARDI, D., AND PATEL-SCHNEIDER, P. 2002. *The Description Logic Handbook: Theory, Implementation and Applications*. Cambridge University Press, Cambridge, UK.

BASILI V. R., CALDIERA, G., AND ROMBACH, H. D. 1994. The goal question metric approach. http://wwwagse.informatik.uni-kl.de/pubs/repository/basili94b/encyclo.gqm.pdf

BASKERVILLE, R. 1993. Information systems security design methods: Implications for information systems development. *ACM Comput. Surv. 25*, 4, 375–414.

BREAUX, T. D., VAIL, M. W., AND ANTON, A. I. 2006. Towards regulatory compliance: Extracting rights & obligations to align requirements with regulations. In *Proceedings of the 14th International Conference on Requirements Engineering*. 49–58.

BREAUX, T. D., ANTON, A. I., AND DOYLE, J. 2009. Semantic parameterization: A process for modeling domain descriptions. *ACM Trans. Softw. Engin. Methodol*.

BUCKSHAW, D. L., PARNELL, G. S., UNKENHOLZ, W. L., PARKS, D. L., WALLNER, J. M., AND SAYDJARI, O. S. 2005. Mission oriented risk and design analysis of critical information systems. *Milit. Op. Resear. 10*, 2.

BUTLER, S. A. 2002. Security attribute evaluation method: A cost benefit approach. In *Proceedings of the 24th International Conference on Software Engineering*. 232–240.

CHEW, E., SWANSON, M., STINE, K., BARTOL N., BROWN, A., AND ROBINSON, W. 2008. *Performance Measurement Guide for Information Security*. NIST Special Publication Series, SP 800-55 Rev 1.

CLEVELAND, W. S. 1985. *The Elements of Graphing Data*. Wadsworth Advanced Books and Software.

COMMON CRITERIA. 2006. Common criteria for information technology security evaluation: Part 1 Introduction and General Model, v3.1-rev 1.

CYSNEIROS, L. M. AND LEITE, J. C. S. P. 2004. Nonfunctional requirements: From elicitation to conceptual models. *IEEE Trans. Softw. Engin. 30*, 5.

DAVIS, T. 2005. Federal computer security report card grades of 2004. Press Release. Government Reform Committee.

DOD 5200.28-STD. 1985. Department of Defense trusted computer system evaluation criteria.

DOD 5200.40. 1997. Department of Defense information technology certification and accreditation (DITSCAP), 1997.

DOD 8510.01. 2007. Department of Defense information assurance certification and accreditation process (DIACAP) Instruction.

DODI 8500.2. 2003. IA implementation.

DONZELLI, P. AND BASILI, V. 2006. A practical framework for eliciting and modeling system dependability requirements: Experience from the NASA high dependability computing project. *J. Syst. Softw. 79*, 1, 107–119.

DUQUENNE, V. AND DAVIS, T. 2005. Duquenne, V. Contextual implications between attributes and some representational properties for finite lattices. Beitrage zur Begrisanalyse, B.I. Wissenschaftsverlag. 213–239.

EASTERBROOK, S. 1993. Domain modelling with hierarchies of alternative viewpoints. In *Proceedings of the International Symposium on Requirements Engineering*. 65–72.

ERNST AND YOUNG 2005. Report on the widening gap. 8th Annual Global Information Security Survey.

FEATHER, M. S. AND CORNFORD, S. L. 2003. Quantitative risk-based requirements reasoning. *Require. Engin. J. 8*, 4, 248–265.

GANTER, B. AND WILLE, R. 1996. *Formal Concept Analysis*. Springer.

GEER, D. 2003. Risk management is still where the money is. *IEEE Computer 36*, 12, 129–131.

GENTNER, D. 1983. Structure-mapping: A theoretical framework for analogy. *Cogn. Sci. 7*, 155–170.

GOOD, P. I. AND HARDIN, J. W. 2006. *Common Errors in Statistics (and How to Avoid Them)* 2nd Ed., Chapter 9, Page 135, Wiley-Interscience.

JACKSON, M. 1995. *Software Requirements and Specifications: A Lexicon of Practice, Principles and Prejudices*. Addison, Wesley.

JILANI, L. L., DESHARNAIS, J., AND MILI, A. 2001. Defining and applying measures of distance between specifications. *IEEE Trans. Softw. Engin. 27*, 8, 673–703.

JOHANSSON, E. AND JOHNSON, P. 2005. Assessment of enterprise information security: Estimating the credibility of the results. In *Proceedings of the Symposium on Requirements Engineering for Information Security (SREIS) at RE'05*.

KALFOGLOU, Y., DASMAHAPATRA, S., AND CHEN-BURGER, J. 2004. FCA in knowledge technologies: Experiences and opportunities. In *Proceedings of the 2nd International Conference on FCA*. 252–260.

KIMBELL, J. AND WALRATH, M. 2001. Life Cycle Security and DITSCAP. In *IANewsletter 4*, 2. http://iac.dtic.mil/iatac.

KOTONYA, G. AND SOMMERVILLE, I. 1996. Requirements engineering with viewpoints. *Softw. Engin. J. 11*, 1, 5–18.

KRAMER, J. AND HAZZAN, O. 2006. The role of abstraction in software engineering. In *Proceedings of the International Workshop on Role of Abstraction in Software Engineering at the 28th International Conference on Software Engineering, Shanghai*. ACM, New York, NY, 1–2.

LEE S. W. AND GANDHI, R. A. 2005. Ontology-based active requirements engineering framework. In *Proceedings of 12th Asia-Pacific Software Engineering Conference (APSEC'05)*, IEEE, 481–490.

LEE S. W. AND GANDHI, R. A. 2006. Requirements as enablers for software assurance. *CrossTalk J. Def. Softw. Engin. 19*, 12, 20–24.

LEE S. W. AND RINE, D. C. 2004a. Missing requirements and relationship discovery through proxy viewpoints model. *Int. J. Informatics 3*, 3, 315–342.

LEE S. W. AND RINE, D. C. 2004b. Case study methodology designed research in software engineering methodology validation. In *Proceedings of 16th International Conference on Software Engineering and Knowledge Engineering*. 117–122.

LEE S. W., MUTHURAJAN, D., GANDHI, R. A., YVAGAL, D., AND AHN, G. J. 2006. Building decision support problem domain ontology from natural language requirements for software assurance. *Int. J. Engin 16*, 6, 851–884.

LEE S. W., GANDHI, R. A., AND AHN, G. J. 2007a. certification process artifacts defined as measurable units for software assurance. *Soft. Process: Improv. Pract. 12*, 2, 165–189.

LEE S. W., GANDHI, R. A., WAGLE, S. J., AND MURTY, A. B. 2007b. r-AnalytiCA: Requirements analytics for certification & accreditation. In *Proceedings of 15th IEEE International Requirements Engineering Conference Posters, Demos and Exhibits Session*. 383–384.

LIN, L., YU, E., AND MYLOPOULOS, J. 2003. Security and privacy requirements analysis within a social setting. In *Proceedings of the 11th International Conference on Requirements Engineering*. 151–161.

LIN, L., NUSEIBEH, B., INCE, D., AND JACKSON, M. 2004. Using abuse frames to bound the scope of security problems. In *Proceedings of the 12th International Conference on Requirements Engineering*. 354–355.

MCDERMID, J. A. 2001. Software safety: Where's the evidence? In *Proceedings of the 6th Australian Workshop on Safety Critical Systems and Software*. Australia, 1–6.

MCDERMOTT, J. 2001. Abuse-case-based assurance arguments. In *Proceedings of the 17th Computer Security Applications Conference*. IEEE, 366–374.

MCGRAW, G. 2006. *Software Security: Building Security*. Addison-Wesley.

MEAD, N. R., HOUGH, E., AND STEHNEY, T. 2005. Security quality requirements Engineering (SQUARE) methodology. Tech. rep. (CMU/SEI-2005-TR-009), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

MITCHELL, R. N. 2005. Using DITSCAP regulations to address HIPAA. Advance for Health Information Executives. http://health-information.advanceweb.com/Editorial/Content/Editorial.aspx?CC=57412.

MOFFETT, J. D., HALEY, C. B., AND NUSEIBEH, B. A. 2004. Core security requirements artefacts. Tech. rep. 2004/23, Open University.

PELTIER, T. Facilitated Risk Assessment Process (FRAP). http://www.peltierassociates.com/.

PFLEEGER, C. P. AND PFLEEGER, S. L. 2003. *Security in Computing* 3rd Ed. Prentice-Hall.

PRUD'HOMMEAUX, E. AND SEABORNE, A. 2006. SPARQL Query Language for RDF. W3C Working Draft.

ROBINSON, W. N. AND PAWLOWSKI, S. 1998. Surfacing root requirements interactions from inquiry cycle requirements. In *Proceedings of the 6th International Conference on Requirements Engineering*. 82–89.

SALTER, C., SAYDJARI, O., SCHNEIER, B., AND WALLNER. J. 1998. Towards a secure system engineering methodology. In *Proceedings of the New Security Paradigms Workshop*.

SCHEDL, M., KNEES, P., AND WIDMER, G. 2005. Interactive poster: Using CoMIRVA for visualizing similarities between music artists. In *Proceedings of the 16th IEEE Visualization Conference*. 89.

SCHNEIER, B. 2000. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, NY.

SIEMENS UK. 2005. Central Communication and Telecommunication Agency (CCTA) risk analysis and management method (CRAMM) Toolkit, Version 5.1. http://www.cramm.com/.

SINDRE, G. AND OPDAHL, A. 2000. Eliciting security requirements by misuse cases. In *Proceedings of TOOLS Pacific*. 120–130.

SOOHOO, K. J. 2000. How much is enough? A risk-management apporach to computer security. Tech. rep. Consortium for Research on Information Security and Policy (CRISP).

STONEBURNER, G., GOGUEN, A., AND FERINGA, A. 2002. *Risk Management Guide for Information Technology Systems*. NIST Special Publication Series, SP 800-30.

TONELLA, P. 2003. Using a concept lattice of decomposition slices for program understanding and impact analysis. *IEEE Trans. Softw. Engin. 29*, 6.

TONELLA, P. 2005. Reverse engineering of object-oriented code. In *Proceedings of the 27th International Conference on Software Engineering*.

US GAO 04-376. 2004. Agencies need to implement consistent processes in authorizing systems for operation. Report from The US Government Accountability Office.

US GAO 05-700. 2005. Department of homeland security needs to fully implement its security program. Report from The US Government Accountability Office.

US GAO 07-837. 2007. Despite reported progress, federal agencies need to address persistent weaknesses. Report from The US Government Accountability Office.

VAN LAMSWEERDE. 2004. Elaborating security requirements by construction of intentional anti-models. In *Proceedings of the 26th International Conference on Software Engineering*, 148–157.

VAUGHN, R. B., HENNING, R., AND SIRAJ, A. 2002. Information assurance measures and metrics – state of practice and proposed taxonomy. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*. 331–340.

VERDON, D. AND MCGRAW, G. 2004. Risk analysis in software design. *IEEE Secur. Priv. Mag. 2*, 4, 79–84.

VOAS, J. 1999. Certifying software for high-assurance environments. *IEEE Software 16*, 4, 48–54.

WASSON, K. S. 2006. A case study in systematic improvement of language for requirements. In *Proceedings of the 14th International Requirements Engineering Conference*. 6–15.

WILLE, R. 1997. Conceptual graphs and formal concept analysis. In *Proceedings of the International Conference on Conceptual Structures*. 290–303.

WONG, P. C. AND THOMAS, J. 2004. Visual analytics. *IEEE Comput. Graph. Appl. 24*, 5, 20–21.

YIN, R. K. 1994. C*ase Study Research: Design and Methods* 2nd Ed. Applied Social Research Methods Series, 5, Sage Publications.

YUDISTIRA, A., GIORGINI, P., AND MYLOPOULOS, J. 2006. Risk modelling and reasoning in goal models. DIT-06-008, University of Trento.

Received March 2008; revised April 2009; accepted August 2009