Proceedings of the Third International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2009)

Information System Security Compliance to FISMA Standard: A Quantitative Measure

E. Hulitt[1] and R. Vaughn[2]

[1]U.S. Army Engineer Research and Development Center, CEERD-IS, 3909 Halls Ferry Road, Vicksburg, MS 39180-6199, USA
[2]Department of Computer Science and Engineering, Center for Computer Security Research, P.O. Box 9637, Mississippi State University, Mississippi State, MS 39762, USA,
e-mail: [1]Elaine.Hulitt@usace.army.mil, [2]Vaughn@cse.msstate.edu

Abstract

To ensure that safeguards are implemented to protect against a majority of known threats, industry leaders are requiring information processing systems to comply with security standards. The National Institute of Standards and Technology Federal Information Risk Management Framework (RMF) and the associated suite of guidance documents describe the minimum security requirements (controls) for non-national-security federal information systems mandated by the Federal Information Security Management Act (FISMA), enacted into law on December 17, 2002, as Title III of the E-Government Act of 2002. The subjective compliance assessment approach described in the RMF guidance, though thorough and repeatable, lacks the clarity of a standard quantitative metric to describe for an information system the level of compliance with the FISMA-required standard. Given subjective RMF assessment data, this article suggests the use of Pathfinder networks to generate a quantitative metric suitable to measure, manage, and track the status of information system compliance with FISMA.

Keywords

Risk Assessment, Secure Architecture Modelling, Metrics and Architectures

1. Introduction

To ensure that safeguards are implemented to protect against a majority of known threats, industry leaders are requiring that information processing systems comply with specific security standards. The Federal Information Security Management Act (FISMA) enacted into law on December 17, 2002, as Title III of the E-Government Act of 2002 (United States General Accounting Office (USGAO), 2004) defined three security objectives for federal government information systems: (1) Confidentiality, to preserve authorized restrictions on access and disclosure, with means for protecting personal privacy and proprietary information; (2) Integrity, to guard against improper information modification or destruction while ensuring information non-repudiation and authenticity; and (3) Availability, to ensure timely and reliable access to and use of information (United States Public Law 107-347-DEC. 17 2002, 116 STAT. 2899). To achieve these security objectives, FISMA tasked the National Institute of Standards and Technology (NIST) to develop a set of

standards and guidelines, the Federal Information Risk Management Framework (RMF) (Figure 1), that (1) describe categories for information systems according to risk levels (low, moderate, high), (2) identify types of information systems to be included in each category, and (3) describe a minimum set of security requirements (controls) that must be applied to systems in each category to achieve adequate security (NIST, 2004; USGAO, 2004). Adequate security is defined by United States Office of Management and Budget (OMB) Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information" (OMB, 1996). FISMA also requires an annual assessment of information system compliance with the standard (NIST, 2003). With approximately 100 security controls in the low-impact category to over 300 security controls in the high-impact category, the subjective compliance assessment approach described in the RMF guidance, though thorough and repeatable, lacks the clarity of a standard quantitative metric to describe for an information system the level of compliance with the standard. Given the review process outlined by NIST RMF documents, the challenge is to provide a quantitative risk analysis metric adequate to (1) clearly describe the status of compliance with the FISMA-required standard, (2) track progress toward compliance with the FISMA-required standard, (3) direct the allocation of resources required to meet FISMA minimum requirements, and (4) simplify annual report preparation. The authors propose generating a quantitative risk analysis metric at the information system level, using Pathfinder networks (PFNETs), to measure, manage, and track the status of system security compliance with the FISMA-required standard.

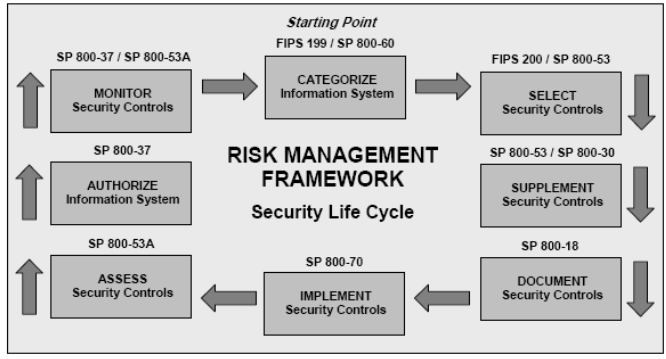

Figure 1: Risk management framework (NIST 2006b)

2. The RMF

The RMF, shown in Figure 1, describes the steps and related standards and guidelines for implementing the minimum set of controls required to provide adequate security for an information system and the associated information stored, processed, and transmitted by that system. The framework includes guidance for assuring that controls are properly implemented and operating as intended to provide the expected security benefit. The RMF emphasizes the idea that risk management is a continuous process.

2.1. Federal Information Processing Standard 199

Federal Information Processing Standard (FIPS) 199 (NIST, 2004) addresses the first two FISMA mandates, the definition of information system categories according to risk level and the identification of system types to include in each category. FIPS 199 defines three categories for information systems considering the potential impact to organizations and individuals should a breach of confidentiality, integrity, or availability occur: (1) Low, limited adverse effect, (2) Moderate, serious adverse effect, and (3) High, severe or catastrophic adverse effect. FIPS 199 applies to all federal information systems except those designated as national security as defined in 44 United States Code Section 3542(b)(2).

2.2. FIPS 200

FIPS 200 (NIST 2006a) addresses the third FISMA mandate, to develop minimum information security requirements (controls) for information systems in each category as defined by FIPS 199. FIPS 200 went into effect when published, March 2006. Federal agencies are required to be in compliance with the standard no later than 1 year from its effective date. There is no provision under FISMA for waivers to FIPS 200.

2.3. FISMA-required System Controls

As required by FIPS 200, NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems* (NIST, 2006b), defines the security controls and provides guidelines for selecting the appropriate set to satisfy the minimum requirement for adequate security given a system category of low, moderate, or high impact. The control sets described in FIPS 200 cover 17 security-related areas (families). As illustrated in Table 1, the 17 security control families are organized into three classes—management, operational, and technical—to facilitate the selection and specification of controls when evaluating an information system.

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Table 1: Security control classes, families, and identifiers (NIST, 2006b)

Two-character identifiers are assigned to each control family. A number is appended to the family identifier to uniquely identify controls within each family. Appendix D of SP 800-53 identifies three minimum sets (baselines) of security controls that correspond to the low-, moderate-, and high-impact information system categories defined in FIPS 199. Appendix F of SP 800-53 provides a detailed description of each security control and numbered enhancements for each control where applicable. As illustrated in Table 2, controls in the Access Control family not used in a particular baseline are marked "Not Selected". The numbers in parentheses following the control identifiers indicate the control enhancement that applies. The baselines are intended to be broadly applicable starting points and may require modification to achieve adequate risk mitigation for a given system (NIST, 2006b).

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)

Table 2: Excerpt from security control baselines (NIST, 2006b)

3. Compliance Measurement Using PFNETs

PFNETs are the result of an effort by Dearholt and Schvaneveldt (1990) to develop network models for proximity data (Schvaneveldt, 1990b). Proximity refers to the measure of relationship (similarity, relatedness, dissimilarity, distance, etc.) between two entities (Dearholt and Schvaneveldt, 1990). In networks, proximity measures are represented by distance, with small values representing similarity or a high level of relatedness, and large values representing dissimilarity or a low level of relatedness

(Dearholt and Schvaneveldt, 1990). Given a dissimilarity matrix resulting from the subjective categorization (mapping) of entities as defined by Dearholt and Schvaneveldt (1990), application of the Pathfinder algorithm generates a unique quantitative network representation of the proximity data. Any change in the subjective categorization of entities—in the case of risk analysis, vulnerabilities to threats—changes the resulting network. Our research indicates that the Pathfinder technique may be suitable for generating quantitative network models of information security standard controls—more accurately, the lack thereof—and information system security controls for comparison using a correlation coefficient (*cc*) formula to determine the status of information system compliance with a specified standard (*%compliant*). The building of a PFNET involves the following steps (Kudikyala, 2004):

1) Correlate entities (e.g., vulnerabilities to threats) in an *n* x *n* matrix.
2) Build entity co-occurrence groups from entity correlations.
3) Build similarity matrix from co-occurrence groups.
4) Build dissimilarity matrix from similarity matrix.
5) Apply Pathfinder algorithm to dissimilarity matrix to build PFNET.
6) Build minimum distance matrix from PFNET.
7) Assuming steps 1 through 6 are followed to build two models of the same data entities as perceived by two different stakeholders, use a *cc* formula to determine the degree of covariance (similarity) between the two models – quantitatively measure the similarity between two perceptions of the relationship between the same set of data entities.

As illustrated in Figure 2, to generate the proposed *%compliant* metric, the researcher must

- Define a representative threat set where the threat level of detail is dependent on the stakeholder (e.g., system security analyst or FISMA security certifier) requirements.
- Build an *open-risk* PFNET model of the FISMA-required standard security controls. Controls when negated become vulnerabilities. Map all vulnerabilities to threat set. Complete the Pathfinder procedure.
- Build a *current-risk* PFNET model of the information system being evaluated. Map system current vulnerabilities to the threat set–mapping defined by the open-risk model (the standard). Complete the Pathfinder procedure.
- Generate current- and open-risk minimum-distance matrices from the PFNETs generated. Compare the minimum distance matrices using a *cc* formula to generate overall *%similar* measures for the models as well as detailed *%similar* measures for each entity within the models.
- Subtract the overall *cc %similar* to open-risk measure from 1 to generate the *%compliant* to *closed-risk* (no vulnerabilities) measure.

Assuming we are evaluating a Financial Management System (FMS) that is web-enabled, intranet accessible, and categorized as moderate impact using the NIST criteria, an example using the Pathfinder technique follows.

3.1. Define Representative Threat Set

Table 3 is a sample list of threats associated with operating the FMS application. The threat categories are taken directly or derived from Ozier (2004), Bishop (2003), and the *Federal Information System Controls Audit Manual* (FISCAM) (USGAO, 1999).

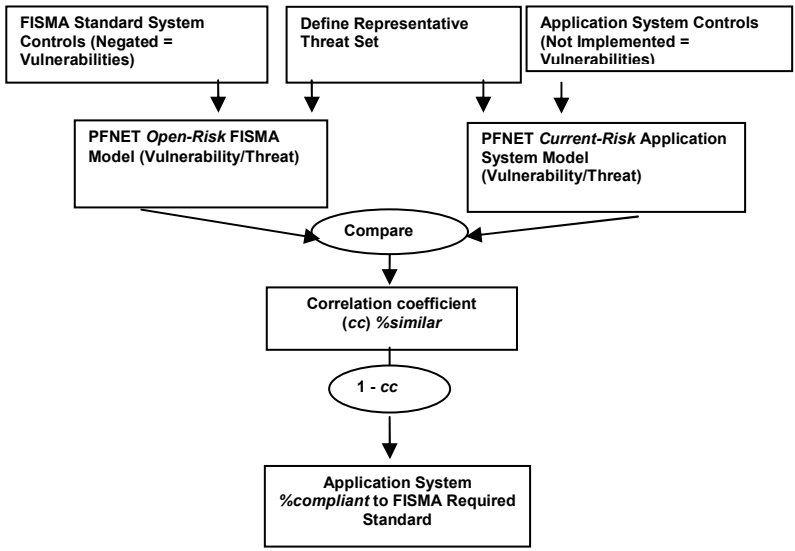

Figure 2: Compliance measurement using Pathfinder

3.2. Build *open-risk* PFNET Model

Table 4 contains a subset of the FISMA-required baseline controls for a moderate-impact system. In Table 5, the controls from Table 4 are negated to create the vulnerability set for this example. To build the open-risk model (open standard) for evaluation of the FMS system, we assume all 20 vulnerabilities (low-level categories) exist by mapping/relating them to the 9 threats (high-level categories) identified in Table 3. Vulnerabilities may be mapped to more than one threat. For this example, vulnerabilities were related to threats resulting in the co-occurrence groups shown in Table 6.

A software tool was used to build an n x n similarity matrix of distinct entities categorized. For this example, n is the sum of 9 threats and 20 vulnerabilities resulting in a 29 x 29 similarity matrix for the open-risk co-occurrence groups. Similarity matrix entries reflect the number or times grouped entities co-occur. For the standard open-risk co-occurrence groups, shown in Table 6, V8 and V4 co-occur 4 times. In the open-risk similarity matrix, the co-occurrence count at entries (V8,

V4) and (V4, V8) would be 4. Higher co-occurrence counts indicate greater similarity. A software tool was used to build a dissimilarity matrix from the similarity matrix of categorized entities. The vulnerability-to-threat relationships in this example are symmetric. Therefore an open-risk dissimilarity matrix (upper triangular portion only) is generated from the open-risk similarity matrix by subtracting each co-occurrence count entry from the maximum co-occurrence count entry plus one to prevent 0-value dissimilarity matrix entries. Lower co-occurrence counts indicate greater similarity.

ID	Threat Category Name
T1	Introduction of Unapproved Software
T2	Software Version Implementation Errors
T3	Sabotage of Software
T4	Theft of Software
T5	Sabotage of Data/Information
T6	Theft of Data/Information/Goods
T7	Destruction of Data/Information
T8	Disruption of Service
T9	Accountability Data Loss

Table 3: Threat categories

ID	FISMA Control Name
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-5	Separation of Duties
AC-7	Unsuccessful Login Attempts
AC-8	System Use Notification
AC-13	Supervision and Review – Access Control
AU-2	Auditable Events [Access]
AU-6	Audit Monitoring, Analysis, and Reporting
CM-1	Configuration Management Policy and Procedures
CM-5	Access Restrictions for Change
CP-4	Contingency Plan Testing and Exercises
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
IA-2	User Identification and Authentication
PS-4	Personnel Termination
SA-5	Information System Documentation [Operations]
SC-2	Application Partitioning
SC-8	Transmission Integrity
SI-9	Information Input Restrictions

Table 4: FISMA standard control subset (NIST, 2006b)

A software tool, applying the Dearholt and Schvaneveldt algorithm, was used to generate the open-risk PFNET from the dissimilarity matrix. A path will exist between node pair (i, j) in PFNET (r, q) if and only if there is no shorter alternate path between (i, j), where r is the Minkowski r-metric calculation of path weight, for paths with number of links $\leq q$.

The distance between two nodes not directly linked is computed using the Minkowski *r*-metric. For path *P* with weights w_1, w_2, ..., w_k, the Minkowski distance is (Dearholt and Schvaneveldt, 1999; Kudikyala, 2004)

$$w(P) = \left(\sum_{i=1}^{k} w_i^r \right)^{1/r} \quad \text{where } r \geq 1,\ w_i \geq 0 \text{ for all } i. \qquad (1)$$

When $r = 1$, path weight is calculated by summing the link weights along the path (Dearholt and Schvaneveldt, 1990; Kudikyala, 2004). Calculating path weight this way assumes ratio-scale data where each weight value is presumed to be within a multiplicative constant of the "correct" value (Dearholt and Schvaneveldt, 1990). When link values are obtained from empirical data, computing path weight this way may not be justifiable (Schvaneveldt, 1990a). For generating PFNETs, where only the ordinal relationships between link weights and path weights are important, *r* should be set to ∞ (Dearholt and Schvaneveldt, 1990). When $r = \infty$, the path weight is the same as the maximum weight associated with any link along the path (Dearholt and Schvaneveldt, 1990; Kudikyala, 2004).

The PFNET generated from the open-risk dissimilarity matrix is a mathematical model of standard open risk.

Control ID	Vulnerability ID	Vulnerability Category Name
CM-1	V1	Inadequate Configuration Management Policy and Procedures
CM-5	V2	Inadequate Access Restrictions for Change
AC-3	V3	Inadequate Access Enforcement
IA-2	V4	Inadequate User Identification and Authentication
AC-2	V5	Inadequate Account Management
AC-8	V6	No System Use Notification
AC-7	V7	No Termination After Maximum Unsuccessful Login Attempts
AC-1	V8	Inadequate Access Control Policy and Procedures
AC-13	V9	Inadequate Supervision and Review – Access Control
PS-4	V10	Inadequate Execution of Personnel Termination Procedure
AU-2	V11	Inadequate Access Monitoring
SA-5	V12	No Information System Operations Manual
CP-9	V13	Insufficient System Backups
CP-10	V14	Inadequate Recovery Mechanisms
CP-4	V15	No Contingency Plan Testing and Exercises
AU-6	V16	Inadequate Audit Monitoring, Analysis
SC-8	V17	Integrity of Transmitted Data not Protected
AC-5	V18	Inadequate Separation of Duties
SC-2	V19	Inadequate Application Partitioning
SI-9	V20	Inadequate Information Input Restrictions

Table 5: Vulnerability categories

(T1,V1)
(T2,V1)
(T3,V2)
(T4,V2)
(T5,V18,V17,V10,V8,V4,V3,V1)
(T6,V18,V10,V8,V4,V3,V1)
(T7,V20,V19,V10,V8,V4,V3,V1)
(T8,V15,V14,V13,V12,V3,V1)
(T9,V16,V11,V9,V8,V7,V6,V5,V4)

Table 6: Standard open-risk co-occurrence groups

3.3. Build *current-risk* PFNET Model

Assume these vulnerabilities exist in the FMS system: V4, V6, V7, V8, V9, V10, V11, V12, V13, V14, V15, V16, V17, V18, V19, and V20 (see Table 5). To build the current-risk PFNET model, map the FMS vulnerabilities to threats as dictated by the vulnerability mappings in the open-risk standard model to generate the co-occurrence groups shown in Table 7 under "FMS System Current Risk." (Note: the Standard Open Risk and FMS System Current Risk co-occurrence groups in Table 7 are the initial entries in Table 8.)

Standard Open Risk	FMS System Current Risk
(T1,V1)	
(T2,V1)	
(T3,V2)	
(T4,V2)	
(T5,V18,V17,V10,V8,V4,V3,V1)	(T5,V18,V17,V10,V8,V4)
(T6,V18,V10,V8,V4,V3,V1)	(T6,V18,V10,V8,V4)
(T7,V20,V19,V10,V8,V4,V3,V1)	(T7,V20,V19,V10,V8,V4)
(T8,V15,V14,V13,V12,V3,V1)	(T8,V15,V14,V13,V12)
(T9,V16,V11,V9,V8,V7,V6,V5,V4)	(T9,V16,V11,V9,V8,V7,V6,V4)

Table 7: Co-occurrence groups

Open Risk:	(T1,**V1**)	(T2, **V1**)
See Table 7	(T3,**V2**)	(T4,**V2**)
	(T5,V18,V17,V10,V8,V4,**V3**,**V1**)	(T6,V18,V10,V8,V4,**V3,V1**)
	(T7,V20,V19,V10,V8,V4,**V3**,**V1**)	(T8,V15,V14,V13,V12,**V3,V1**)
	(T9,V16,V11,V9,V8,V7,V6,**V5**,V4)	
FMS Model 1	(T5,V18,**V17**,V10,V8,**V4**)	(T6,V18,V10,V8**,V4**)
See Table 7	(T7,V20,V19,V10,V8,**V4**)	(T8,V15,V14,V13,V12)
	(T9,V16,V11,V9,V8,V7,V6,**V4**)	
FMS Model 2	(T5,**V18**,V10,V8)	(T6,**V18**,V10,V8)
	(T7,**V20,V19**,V10,V8)	(T8,V15,V14,V13,V12)
	(T9,V16,V11,V9,V8,V7,V6)	
FMS Model 3	(T5,**V10**,V8)	(T6,**V10**,V8)
	(T7,**V10**,V8)	(T8,V15,V14,V13,V12)
	(T9,V16,V11,V9,V8,V7,V6)	
FMS Model 4	(T5,V8)	(T6,V8)
	(T7,V8)	(T8,V15,V14,V13,V12)
	(T9,**V16**,**V11**,V9,V8,**V7**,V6)	
FMS Model 5	(T5,V8)	(T6,V8)
	(T7,V8)	(T8,V15,V14,V13,**V12**)
	(T9,**V9**,V8,V6)	
FMS Model 6	(T5,V8)	(T6,V8)
	(T7,V8)	(T8,**V15**,**V14**,**V13**)
	(T9,V8,V6)	
FMS Model 7	(T5,**V8**)	(T6,**V8**)
	(T7**,V8**)	(T9,**V8**,V6)
FMS Model 8	(T9,**V6**)	
Closed Risk	(No Vulnerabilities)	
Note: Vulnerabilities in bold type assumed corrected in following model.		

Table 8: Risk model co-occurrence groups

Using the procedure described in Section 3.2, a similarity matrix is generated from the FMS system current-risk co-occurrence groups, a dissimilarity matrix is generated from the similarity matrix, and the PFNET algorithm is applied to the dissimilarity matrix to generate the current-risk PFNET model.

The PFNET generated from the current-risk dissimilarity matrix is a mathematical model of the FMS system current risk.

3.4. Compare Minimum Distance Matrices

A software tool was used to generate minimum distance matrices from the standard open-risk and FMS system current-risk PFNETs using a shortest path algorithm. Path distances for the minimum distance matrices are calculated the traditional way, by adding link weights along paths between nodes. A correlation tool was used to compare the open- and current-risk minimum distance matrices using the *cc* formula that follows:

$$cc = \frac{\sum (a-\bar{a})(b-\bar{b})}{\sqrt{\sum (a-\bar{a})^2 \sum (b-\bar{b})^2}} \qquad (2)$$

where a is the value of an element in the distance vector of the open-risk minimum distance matrix, $\bar{a}$ is the mean of all the elements in the open-risk distance vector (upper or lower triangular values), b is the value of a corresponding element in the distance vector of the system current-risk minimum distance matrix, and $\bar{b}$ is the mean of all elements in the current-risk distance vector. Normally the *cc* range is [-1, +1], where -1 represents no similarity and +1 represents perfect similarity between models (Kudikyala, 2004). Because of the approach taken in this research to compare current system state to a standard perception of adequate security, the *cc* range is narrowed from [-1, +1] to [0, +1] – no comparison beyond a perfect match.

3.5. Generate *%compliant* Measure

The software tool used to compare models generates an overall *cc* value that indicates the degree of covariance (similarity) between the standard open-risk model and the system current-risk model – similarity to unacceptable risk; all vulnerabilities exist. The goal for the FMS system is a *cc* of 0, i.e., no similarity to the open-risk model. Subtracting the overall *cc* value from 1 yields a value (*%compliant)* that indicates how close the FMS system is to standard compliance as defined by the closed-risk model – no vulnerabilities exist. Comparing the FMS system current-risk model 1 to the open-risk model results in a *cc* of 0.45 (see Table 9, "Overall Path Distance *cc*" for FMS 1). The FMS 1 current-risk model in this example exhibits 45 percent similarity to the open-risk model. Subtracting 0.45 from 1.0 (open-risk) yields a value that indicates the FMS system is 55 percent compliant to closed-risk (see Table 9, "*%compliant*" for FMS 1). The more existing vulnerabilities identified in the FMS system, the closer the resulting *cc* value will be to 1.0 (open-risk). As

vulnerabilities are removed, the *cc* value moves closer to 0.0 (closed-risk). Table 8 shows sample FMS risk model co-occurrence groups. The vulnerabilities in bold type are removed in each successive FMS model. For each FMS model, the Pathfinder procedure was applied to generate a minimum distance matrix for comparison with the open-risk model minimum distance matrix. Table 9 shows the overall path distance *cc*, node path distance (detailed) *cc*, and *%compliant* values for the FMS models as vulnerabilities are removed and the FMS models are compared with the open-risk model.

	Open Risk	**FMS 1**	**FMS 2**	**FMS 3**	**FMS 4**	**FMS 5**	**FMS 6**	**FMS 7**	**FMS 8**	**Closed Risk**
%compliant	0.0	0.55	0.59	0.66	0.69	0.77	0.82	0.87	0.95	1.0
Overall Path Distance *cc*	1.0	0.45	0.41	0.34	0.31	0.23	0.18	0.13	0.05	0.0
Node Path Distance *cc*										
V1	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V2	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V3	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V4	1.0	0.70	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V5	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V6	1.0	0.43	0.46	0.45	0.62	0.41	0.33	0.33	0.23	0.0
V7	1.0	0.43	0.46	0.45	0.62	0.0	0.0	0.0	0.0	0.0
V8	1.0	0.70	0.43	0.35	0.13	0.10	0.09	0.09	0.0	0.0
V9	1.0	0.43	0.46	0.45	0.63	0.41	0.0	0.0	0.0	0.0
V10	1.0	0.75	0.54	0.43	0.0	0.0	0.0	0.0	0.0	0.0
V11	1.0	0.43	0.46	0.45	0.63	0.0	0.0	0.0	0.0	0.0
V12	1.0	0.56	0.56	0.56	0.56	0.56	0.0	0.0	0.0	0.0
V13	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
V14	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
V15	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
V16	1.0	0.43	0.46	0.45	0.62	0.0	0.0	0.0	0.0	0.0
V17	1.0	0.66	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V18	1.0	0.74	0.69	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V19	1.0	0.65	0.62	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V20	1.0	0.65	0.62	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T1	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T2	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T3	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T4	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T5	1.0	0.66	0.64	0.54	0.29	0.29	0.29	0.29	0.0	0.0
T6	1.0	0.64	0.61	0.51	0.31	0.31	0.31	0.31	0.0	0.0
T7	1.0	0.64	0.62	0.55	0.29	0.29	0.29	0.29	0.0	0.0
T8	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
T9	1.0	0.43	0.46	0.45	0.62	0.41	0.33	0.33	0.23	0.0

Table 9: Risk model comparisons

Using the distance vectors for each entity in the minimum distance matrices for the open- and current-risk models, detailed *cc* values are generated that indicate how a single entity in each model relates to all others – how a single entity contributes to the similarity between models. An analysis of the detailed *cc* values for information system current risk models compared to the standard open-risk model should provide

some insight with regard to choosing an efficient mitigation path for achieving compliance with the FISMA standard – *%compliant* = 1.0; no vulnerabilities exist. Live data experiments are being conducted where the following methods for choosing an efficient mitigation path will be compared:

1. Remove vulnerabilities related to the threat with the highest Node Path Distance *cc* value.
2. Remove top 25% of remaining vulnerabilities based on highest Node Path Distance values.
3. A Combination of methods 1 and 2.

4. Conclusion

Technical Topic Area 3 (TTA 3), Cyber Security Metrics, of the Department of Homeland Security Broad Agency Announcement (BAA), Cyber Security Research and Development (BAA07-09) (United States Department of Homeland Security (USDHS), 2007), describes security metrics as "a difficult, long-standing problem." TTA 3 cites the fact that the security metrics problem is listed on the INFOSEC Research Council (IRC) Hard Problems List (IRC, 1999) as evidence of the importance of research in this area. Good security metrics are required to direct the allocation of security resources to improve the security status of government information systems, to demonstrate compliance with FISMA-required security standards, and to simplify the annual FISMA reporting requirement. TTA 3 advises that "the lack of sound and practical security metrics is severely hampering progress both in research and engineering of secure systems" (USDHS, 2007).

The proposed approach is unique in that it offers a *%compliant* metric at the information system level. The proposed approach in combination with NIST RMF guidance provides for producing consistent quantitative results. Detailed *cc* values should indicate vulnerability groups where targeted cost benefit analysis may be applied to determine an effective approach for eliminating vulnerabilities contributing most to the noncompliant state of the system being evaluated. The quantitative *%compliant* metric should allow for the discussion of system compliance with FISMA-required standards in terms easily understood by participants at various levels of an organization without requiring all to have detailed knowledge of the internals of the security standard or the system being evaluated.

5. References

Bishop, M. (2003), *Computer Security: Art and Science,* Addison-Wesley, Boston, Massachusetts, ISBN: 0-201-44099-7.

Dearholt, D. W., and Schvaneveldt, R. W. (1990), “Properties of Pathfinder networks”, in Schvaneveldt, R. W. (Ed.) *Pathfinder Associative Networks: Studies in Knowledge Organization*, Ablex Publishing Corporation, Norwood, New Jersey, pp. 1-30, ISBN: 0-89391-624-2.

INFOSEC Research Council (IRC) (1999), "National scale INFOSEC research hard problems list", Draft 21, http://www.infosec-research.org/documents (Accessed September 1999).

Kudikyala, U. K. (2004), "Reducing misunderstanding of software requirements by conceptualization of mental models using Pathfinder networks", Ph.D. dissertation, Department of Computer Science, Mississippi State University, Starkville, Mississippi.

National Institute of Standards and Technology. (2006a), *Minimum Security Requirements for Federal Information and Information System,* FIPS PUB 200, Gaithersburg, MD USA: Computer Security Division, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

National Institute of Standards and Technology. (2006b), *Recommended Security Controls for Federal Information Systems,* SP 800-53 Rev. 1, Gaithersburg, MD USA: Computer Security Division, http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.

National Institute of Standards and Technology. (2003), *Security Metrics Guide for Information Technology Systems,* SP 800-55, Computer Security Division, Gaithersburg, MD USA: Computer Security Division, http://csrc/nist/gov/publications/nistpubs/800-55/ sp800-55.pdf.

National Institute of Standards and Technology. (2004), *Standards for Security Categorization of Information Systems,* FIPS PUB 199, Gaithersburg, MD USA: Computer Security Division, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Ozier, W. (2004), "Risk analysis and assessment", in Tipton, H. F., and Krause, M. (Ed.) *Information Security Management Handbook*, 5th ed., Auerbach Publications, Boca Raton, Florida, pp795-820, ISBN: 0-8493-1997-8.

Schvaneveldt, R. W. (1990a), "Graph theory and Pathfinder primer", In Schvaneveldt, R. W. (Ed.) *Pathfinder Associative Networks: Studies in Knowledge Organization*, Ablex Publishing Corporation, Norwood, New Jersey, pp297-299, ISBN: 0-89391-624-2.

Schvaneveldt, R. W. (1990b), "Preface", In Schvaneveldt, R. W. (Ed.) *Pathfinder Associative Networks: Studies in Knowledge Organization*, Ablex Publishing Corporation, Norwood, New Jersey, p. ix, ISBN: 0-89391-624-2.

United States Department of Homeland Security. (2007), *Cyber Security Research and Development*, Broad Agency Announcement BAA07-09, pp9-10, http://www.hsarpabaa.com/Solicitations/BAA0709_CyberSecurityRD_Posted_05162007.pdf.

United States General Accounting Office. (1999), *Federal Information System Controls Audit Manual (FISCAM)*, Volume I – Financial Statement Audits, (GAO/AIMD-12.19.6), Accounting and Information Management Division.

United States General Accounting Office. (2004), *Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operations,* Report to Congressional Requesters*,* GAO-04-376, http://www.gao.gov/cgi-bin/getrpt?GAO-04-376.

United States Office of Management and Budget. (1996), *Security of federal automated information resources*, Appendix III to OMB Circular No. A-130, Management of Federal Information Resources, http://www.whitehouse.gov/omb/circulars/a130/ a130.html.

United States Public Law 107-347-DEC. 17 2002, 116 STAT. 2899, *Federal Information Security Management Act (FISMA)*, Title III of the E-Government Act of 2002. http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf, 2002.