Overview of Enterprise Information Needs in Information Security Risk Assessment

Matus Korman, Mathias Ekstedt
Royal Institute of Technology, KTH
100 44 Stockholm, Sweden
Email: {matusk, mathiase}@ics.kth.se

Teodor Sommestad, Jonas Hallberg, Johan Bengtsson
Swedish Defence Research Agency, FOI
583 30 Linköping, Sweden
Email: {teodor.sommestad, jonas.hallberg, johan.bengtsson}@foi.se

***Abstract*—Methods for risk assessment in information security suggest users to collect and consider sets of input information, often notably different, both in type and size. To explore these differences, this study compares twelve established methods on how their input suggestions map to the concepts of ArchiMate, a widely used modeling language for enterprise architecture. Hereby, the study also tests the extent, to which ArchiMate accommodates the information suggested by the methods (e.g., for the use of ArchiMate models as a source of information for risk assessment). Results of this study show how the methods differ in suggesting input information in quantity, as well as in the coverage of the ArchiMate structure. Although the translation between ArchiMate and the methods' input suggestions is not perfect, our results indicate that ArchiMate is capable of modeling fair portions of the information needed for the methods for information security risk assessment, which makes ArchiMate models a promising source of guidance for performing risk assessments.**

I. Introduction

Managing information security has become an integral part of enterprise IT governance. Even more so in larger enterprises with complex landscapes of IT systems and higher dependence on automated information processing. In fact, having a systematic process for managing information security has become a regulatory requirement [1]. Management of information security strives to ensure that critical assets are kept free from danger—that those otherwise vulnerable ones are protected in a sufficient and cost-effective manner [2]. Such assets (e.g., having fresh and accurate information, effective business services, well-functioning IT infrastructure, thriving and motivated employees, adequate trust and goodwill, etc.) may stretch all across an enterprise and its boundaries. Protecting assets of an enterprise is a complex task, rich on trade-offs and pitfalls [3]. Hence, effectively managing information security requires making informed decisions.

Risk management is seen as a major and critical part of information security governance, in fact, enterprise governance as such [3]. Risk assessment, risk management's analytical part, is an ultimate tool supporting risk treatment, the executive part of risk management. The former strives to map the landscape of assets, threats, vulnerabilities and risks, while the latter strives to make informed decisions on controlling these landscapes (e.g., by applying countermeasures like installing firewalls, hardening existing systems, adopting new operational procedures, relocating exposed assets to a safer environment, insuring against incidents, etc.). Today, dozens of methods tailored specifically for assessing and managing information security risk exist (see [4], [5], also table I). Most of the methods prescribe a similar process that leads to establishing a scope of the assessment, collecting information, producing intermediary information, and finally quantifying and sorting items such as assets, vulnerabilities, threats and risks, according to a set of parameters. The methods however differ from each other in terms of the target community, details of the analytic process, as well as the information they prescribe or suggest to gather as input. Following a systems theoretic perspective [6], a method can produce accurate results if (a) it is used in appropriate context (e.g, it is well-suited for the type of enterprise given); (b) the process is valid and reliable (i.e., the usage and the "internals" of a method); and (c) inputs to the process are valid and sufficient (i.e., the information that the assessment process takes in). Much as for the analytic process, it is assumable that the spectrum and quality of the input information has a non-negligible impact on the accuracy of the assessment outcome. It also impacts the cost of performing such a risk assessment, as some information may be cheaper to collect (e.g., list of customers), while other may be more costly (e.g., maps of all network cables in an organization). Luckily, the need to gather such information might be reduced through having information security risk management reuse the information gathered within other parts of IT governance. Enterprise architecture [7] attempts to document the essentials of IT and business environments, enable their analysis, and so aid various governance processes. Alignment between methods for information security risk assessment and frameworks for enterprise architecture, might therefore improve the efficiency of information security risk management, and hence IT governance.

Motivated by diffuse suggestions of input information by the different risk assessment methods, this study attempts to describe and compare the methods on what input information they suggest users to collect. Additionally, motivated by the questionable extent of compatibility of the terms describing the methods' input information with the terms describing enterprise architecture, the study attempts to evaluate the ease of matching the former to the latter. The study presents a review of twelve well-established risk assessment methods, addressing the primary research question: *What information do information security risk assessment methods suggest users to collect?* The question is answered using the concepts and structure of ArchiMate [7], [8], a widely adopted general-purpose enterprise architecture modeling language. In addition, the study poses a secondary research question: *To what extent can ArchiMate aid information security risk assessments?* The question is answered in terms of the ease of mapping the suggested input information to the concepts of ArchiMate.

The article unfolds as follows. First, related work is presented, followed by a method of the study and conceptual framework. Subsequently, results are presented, followed by analysis and a discussion.

II. Related work

Existing methods for information security risk assessment differ in features, as well as they are established and tested to different extent. Although multiple studies comparing such methods in different terms such as the analytical process were found, none of the studies comprehensively compare such methods in terms of input suggestions (e.g., their richness, completeness or balance with regards to a predefined structure such as the enterprise architecture language ArchiMate can provide).

Shamala et al. [9] studied six methods (CRAMM, CORAS, OCTAVE, ISRAM, Risk Analysis based on Business Model, and NIST SP 800-30) and compared them on a number of features. Besides a general category of information related to operational/business function, whether the methods use information about critical assets, and seven different categories of assets (data, software, information, physical, personnel, hardware and facility assets), the study did not compare the methods on what input information they suggest users to collect. ENISA [10] provides a benchmark of four methods (IT-Grundschutz, NIST SP 800-30, Dutch A&K Analysis and the to-date withdrawn ISO/IEC 17799:2005), namely of their processes, inputs and outputs. The benchmark, however, provides a list of input items rather than a unified picture of what type of information the methods suggest as input. Macedo [5] introduces to risk assessment as such, compares and further describes a number of methods. Although the study also describes inputs to the risk assessment process, it does so briefly and on overall. Syalim et al. [11] studied four methods (Mehari, Magerit, NIST SP 800-30, and Microsoft's Security Management Guide) regarding the analytic process, recommendation of countermeasures, and documentation. However, the comparison focuses on the flow the analytic process, and omits input information. Fenz & Ekelhart [12] study suitability of methods for verification, validation and evaluation of different phases of five risk assessment methods (CRAMM, NIST SP 800-30, OCTAVE, EBIOS and ISO/IEC 27005). A somewhat similar study, Giannopoulos et al. [13], describes a set of methods for risk assessment for critical infrastructure, however, with regards to security in general, not specifically information security. The thesis of Johansson [14] discusses methods for prioritizing data collection during security assessments, based on the content of established standards for information security. However, it does not give any rich description of how the prioritization is done in established security risk assessment methods. There is more work that presents methods and frameworks for assessing information security risk, which is rooted in the ideas presented in established frameworks, and describes information to collect. For instance, Cyber Security Modeling Language (CySeMoL) [15] used literature and domain experts to identify concepts of relevance for cyber security assessments. However, CySeMoL is a solution for vulnerability assessment, not a solution for comprehensive risk assessment.

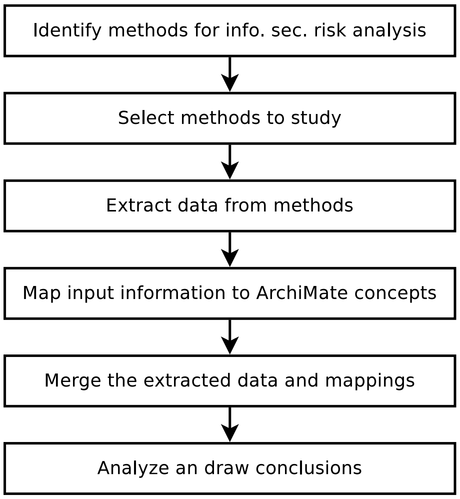
Identify methods for info. sec. risk analysis
Select methods to study
Extract data from methods
Map input information to ArchiMate concepts
Merge the extracted data and mappings
Analyze an draw conclusions

Figure 1. Stages of the study method

On the integration between information security risk assessment and enterprise architecture modeling, Grandry et al. [16] suggested a scheme for conceptual mapping of a set of terms used in information security risk management to ArchiMate. Szwed & Skrzyński [17] used ArchiMate in context of information security risk assessment, although rather indirectly, only to capture the added value tree of assets in an IT architecture.

III. Method

The study proceeded in six stages as outlined in Fig. 1 and detailed below. During the study, no special equipment was used besides common office applications and the R programming environment for statistics and plotting.

First, a broad set of methods was identified using existing reviews of risk assessment methods (e.g. [4], [5]), online search engines (e.g., Google), and online library services, aiming to identify existing methods applicable to information security risk assessment. Keywords included terms such as “risk assessment”, “risk analysis”, “method” and “information security”. A total of seventy-six candidate publications were found. However, only a subset rendered as actual for the study, as discussed below.

Second, the broad set of identified methods was reduced according to the following set of criteria. For a method to be selected, it had to be available free of charge (unlike e.g. CRAMM [18], also in [5]), applicable to information security and assessment of information systems (unlike e.g. COUNTERACT [19]), and the method documentation had to be available in a language, which at least two among the authors could reliably and efficiently understand, i.e., English, Swedish or Norwegian language (unlike e.g. EBIOS [20]). An initial selection yielded a list of twenty-four methods. Subsequently, each selected method had to contain a method or process description, and suggest input information. Furthermore, the methods had to be in use. This selection criterion was adopted to exclude methods that have been proposed but

Table I. RISK ASSESSMENT METHODS INCLUDED IN THE STUDY

Short name	Full name	Pages	Life-cycle	Ref.
Grundschutz	BSI-Standard 100-3 Risk analysis based on IT-Grundschutz	23	P, E	[23]
TRA-1	Harmonized Threat and Risk Assessment Methodology	290	P, E	[24]
TRITF	The Risk IT Framework	107	P, E	[25]
CORAS	CORAS	456	P, E	[26]
ISO/IEC 27005	ISO/IEC 27005 Information technology – Security techniques – Information security risk management	76	P, E	[27]
MEHARI	Methode Harmonisée d'Analyse de Risque	46	E	[28]
TSRMG	The Security Risk Management Guide	129	P, E	[29]
MAGERIT	Methodology for Information Systems Risk Analysis and Management	267	P, E	[30]
OCTAVE	The Operationally Critical Threat, Asset, and Vulnerability Evaluation	1113	E	[31]
MG-3	A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems	73	P, E	[32]
NIST RMF	NIST Risk Management Framework	1142	P, E	[33]
HMG IA	HMG IA Standard No. 1 Technical Risk Assessment	114	P, E	[34]

Note: In the column life-cycle (of a system), P stands for planned, E for existing.

likely not used, and which might thus lack the refinement accomplished through revisions based on experience on the use of a method. In practice, this selection criterion was considered to be fulfilled by methods provided by agencies (e.g., NIST) or standardization bodies (e.g., ISO), or methods being often referred to by academic citations, hits by Google Scholar, and hits by general Google search. An example method that did not fulfill those requirements was The Open Group's FAIR (Factor Analysis of Risk) [21], [22]. After the selection stage, twelve methods remained for inclusion in the study. The methods are listed in table I.

Third, data was extracted from each selected method, according to two template documents prepared previously within the study. The first template covered broad information about a method such as publisher, number of pages, target audience and scope, threat information used, data collection process, notations and definitions of basic risk terms, and scales used for assessment parameters. Most importantly in terms of the research question, the first template contained a list of input information used by a method. The second template served for mapping types of input information to concepts defined and used by the ArchiMate modeling language version 2.0 [8]. The process of data extraction was developed by four reviewers and externally reviewed by a person with research experience in the field of information security. Each field of the template was named and commented in text (e.g., *suggested sources of information* commented by "If the document suggests that certain sources of information should be used (e.g., the IT department), list them here"). Before the extraction procedure started, a dry run was carried out on two methods, to make sure that all reviewers interpreted the fields in the same way. Subsequently, the researchers skimmed through the method documents to identify and agree upon parts of them described inputs used in the risk assessment process. Finally, within the data extraction process, each method document was processed independently by two different researchers, to reduce the amount of bias introduced by human processing of the method descriptions, interpreting and mapping terms.

Fourth, input information suggested by the methods were mapped to the concepts defined by ArchiMate. For each method, the mapping was carried out independently by the same two researchers who previously extracted data from the method document. The process of mapping, however, was perceived as methodically difficult, since both the terms used by the methods to describe input information are merely mentioned and often not thoroughly described and/or exemplified (e.g. *business assets* or *information system configuration*), and the concepts used by ArchiMate, although defined, still broad or even vague to some extent (e.g., *business object*, see table V). Also, certain terms used by the methods would map to nearly all of the concepts defined by ArchiMate (e.g. *assets*), while some other would map to none (e.g., *furniture* or *power supplies*). Hence, the alignment between the terms of the methods and those of ArchiMate is not perfect. The researchers attempted to address the challenges as follows. In case of such difficult-to-map or overly general terms (e.g., *asset* or *system*), a note was taken and in most cases no mapping was made. In case a term from a method would map to multiple ArchiMate concepts, a multiple such mapping was made. In case of a security-specific term (e.g., *documentation of controls*), a note was taken that the mapping does not preserve security-related information. In case a security-specific term was additionally found difficult to map (e.g., *software vulnerability*), the term was not mapped. In case a term was interpreted as vague (e.g., *external system assumptions*), a qualified guess of what is intended was made, given the context. The mentioned example is considered in light of the statements "Assumptions made about the external systems will affect the context for analyzing potential threat scenarios involving system assets coming from the interface. The assumptions will include any rules associated with connecting to the external system. For example, an external system might be assumed to be a controlled system where the likelihood of threat agents accessing the analyzed system from the external system is very low. However, the connection can only be made if the system being analyzed places several constraints on the connection." [32] (p. 14). Hence, the term was mapped to ArchiMate's *constraint* (cf. table V). Additionally, since human interpretation of broad terms tends to be subjective and uncertain, each mapping was marked with an indicator of confidence (low, medium or high).

Fifth, the data extracted by each researcher from the selected methods were merged into a single extraction template per method. Also, the mapping of input information to ArchiMate terms was merged into a single spreadsheet for each of the selected methods. If a mismatch existed between the reviewers' mappings, or if both reviewers assigned a low confidence score (one or two), the concept and the mapping was additionally discussed between the two reviewers to ensure consistency and higher accuracy of the mapping. In attempt to measure the consistency of individual mappings and hence the amount of bias introduced by human processing, interpretation and synthesis, six indicators were defined and used for each merging of two individual mappings related to the same method. The indicators are summarized in table II.

Sixth, the data was analyzed, interpreted and drawn conclusions from.

Table II. INDICATORS OF MAPPING CONSISTENCY

Identifier	Criterion
I-1	If one reviewer indicated that an item was overly broad (i.e., would map to many ArchiMate concepts, e.g., five and more); the other reviewer also did so for the item.
I-2	If one reviewer indicated that an item was overly broad; the other reviewer indicated no mapping or at most low mapping confidence for the item.
I-3	Both reviewers have indicated high mapping confidence for an item.
I-4	If one reviewer indicated high mapping confidence for an item, the other reviewer has also mapped the item.
I-5	If both reviewers mapped an item differently, one of them has indicated at most low confidence.
I-6	If one reviewer indicated high mapping confidence for an item, the other mapped the item to a concept in the same slot of ArchiMate.

Table III. CONCEPTS OF ARCHIMATE CORE

	Passive structure	Behavior	Active structure
Business layer	Business object Representation Meaning Value Product Contract	Business process/ function/ interaction Business event Business service	Business actor Business role Business collaboration Business interface Location
App. layer	Data object	Application function/ interaction Application service	App. component Application collaboration Appplication interface
Infrastr. layer	Artifact	Infrastructure function Infrastructure service	Node Device Network Communication path Infrastructure interface System software

Table IV. CONCEPTS OF ARCHIMATE EXTENSIONS

Motivation extension	Implementation & Migration extension
Stakeholder Driver Assessment Goal Requirement Constraint Principle	Work package Deliverable Plateau Gap

IV. CONCEPTUAL FRAMEWORK (ARCHIMATE)

To comprehensibly compare the methods' sets of suggested input information, they need to be measured on a unified metric. For this purpose, the study used the structure defined by ArchiMate [8] to measure and compare the methods. Although ArchiMate is not primarily designed with a security mindset, the reason for the choice is ArchiMate's high popularity and spread, its closeness to and compatibility with TOGAF [35], [36], a popular enterprise architecture framework [37], as well as its rich tool support (e.g., Archi, Sparx Enterprise Architect, BiZZdesign Architect). Hence, it can be assumed that large portions of the most essential information about enterprises and their IT architectures, which can aid risk assessments, are available through ArchiMate models.

The core of ArchiMate defines three layers (business, application and infrastructure layer) and per each layer three groups of concepts (passive structure, behavior and active structure), grouped by the concepts' essence. The core layers and groups together form nine slots, each including a set of concepts. The division of ArchiMate core concepts to the nine slots is shown in table III. ArchiMate additionally defines two extensions, the concepts of which are separate from the core—the motivation extension and the implementation & migration extension. The extensions define additional concepts, shown in table IV, which form two additional slots. Hence, there are eleven slots of

Table V. ARCHIMATE VERSION 2.0, CONCEPTS WITH DEFINITIONS

Concept	Definition
Business actor	An organizational entity that is capable of performing behavior.
Business role	The responsibility for performing specific behavior, to which an actor can be assigned.
Business collab.	An aggregate of two or more business roles that work together to perform collective behavior.
Business interface	A point of access where a business service is made available to the environment.
Location	A conceptual point or extent in space.
Business process	A behavior element that has relevance from a business perspective.
Business function	A behavior element that groups behavior based on a chosen set of criteria (typically required business resources and/or competences).
Business interact.	A behavior element that describes the behavior of a business collaboration.
Business event	Something that happens (internally or externally) and influences behavior (business process, business function, business interaction).
Business service	A service that fulfills a business need for a customer.
Business object	A passive element that has relevance from a business perspective.
Representation	A perceptible form of the information carried by a business object.
Meaning	The knowledge or expertise present in a business object or its representation, given a particular context.
Value	The relative worth, utility, or importance of a business service or product.
Product	A coherent collection of services, accompanied by a contact/set of agreements, which is offered as a whole to (internal or external) customers.
Contract	A formal or informal specification of agreement that specifies the rights and obligations associated with a product.
App. component	A modular, deployable, and replaceable part of a software system that encapsulates its behavior and data and exposes these through a set of interfaces.
App. collab.	An aggregate of two or more application components that work together to perform collective behavior.
App. interface	A point of access where an application service is made available to a user or another application component.
Data object	A passive element suitable for automated processing.
App. function	A behavior element that groups automated behavior that can be performed by an application component.
App. interaction	A behavior element that describes the behavior of an application collaboration.
App. service	A service that exposes automated behavior.
Node	A computational resource upon which artifacts may be stored or deployed for execution.
Device	A hardware resource upon which artifacts may be stored or deployed for execution.
Network	A communication medium between two or more devices.
Comm. path	A link between two or more nodes, through which these nodes can exchange data.
Infrast. interface	A point of access where infrastructure services offered by a node can be accessed by other nodes and application components.
System software	A software environment for specific types of components and objects that are deployed on it in the form of artifacts.
Infrastr. function	A behavior element that groups infrastructural behavior that can be performed by a node.
Infrastr. service	An externally visible unit of functionality, provided by one or more nodes, exposed through well-defined interfaces, and meaningful to the environment.
Artifact	A physical piece of data that is used or produced in a software development process, or by deployment and operation of a system.
Stakeholder	The role of an individual, team or organization (or classes thereof) that represents their interests in, or concerns relative to, the outcome of the architecture.
Driver	Something that creates, motivates, and fuels the change in an organization.
Assessment	The outcome of some analysis of some driver.
Goal	An end state that a stakeholder intends to achieve.
Requirement	A statement of need that must be realized by a system.
Constraint	A restriction on the way in which a system is realized.
Principle	A normative property of all systems in a given context, or the way in which they are realized.
Work package	A series of actions designed to accomplish a unique goal within a specified time.
Deliverable	A precisely-defined outcome of a work package.
Plateau	A relatively stable state of the architecture that exists during a limited period of time.
Gap	An outcome of a gap analysis between two plateaus.

Table VI. MAPPING OF EACH METHOD'S INPUT INFORMATION TO THE CONCEPTS OF ARCHIMATE

	ArchiMate concept	Method												
		Grundschutz	TRA-1	TRITF	CORAS	ISO/IEC 27005	Mehari	TSRMG	MAGERIT	OCTAVE	MG-3	NIST RMF	HMG IA	*(all together)*
Business layer	Product			1						2				3
	Value		3	6	1	1	3	1		11		1		27
	Representation			1	1	1			3			8		14
	Contract		1	2			1		4	2	1			11
	Business service		1	2			1		2			1		7
	Business interface									1	1	1		3
	Business collaboration					2			1	1				4
	Business object		13	13	2	3	13	4		9	1	1		59
	Business meaning	3	2	3	2	1	4		3			4		33
	Business event			7		2	1	8				1		19
	Business function/process		2	8		5	6		3	4	2	2		32
	Business role		10	1		3	7		12	9	2	2		46
	Business actor		10	2		3	6		10	16	2	6		55
	Location		2			2	3	1	6	2	1	1	1	19
Application layer	Application service			1		2	1		3			3	1	11
	Application interface					1	3			1	4	5		14
	Application collaboration					2	3		1		2	5		13
	Data object		13			1		1	11	1	2	5		34
	App. interaction/function					2				1	5	8		16
	Application component		5			2	3	1	10		2	5		28
Infrastructure layer	Infrastructure service					2	1		10		1	3	2	19
	Infrastructure interface					1	2				2	4		9
	Infrastructure function					2					3	4		9
	Artifact		12			1						2		15
	Node		1			2	3	1	1	5	1	4		18
	Communication path	1				2	1		2	2	1	4		13
	System software		6			2	3		3	3	2	5		24
	Device		10			1	3		18	3	1	5		41
	Network	1				2	3	1	12	5	1	3		28
Motivation extension	Stakeholder					1	1	1				3		6
	Driver		2	8			7	1						18
	Assessment		1	19		3		10			1	1		35
	Goal			1			1							2
	Principle			3			2	1						6
	Requirement	3	2	6			1			6	2	3	1	24
	Constraint	1	1			11	12			6	2	2		35
Migration and impl. extension	Plateau													
	Gap			2		2				1				5
	Deliverable						1							1
	Work package					1			1		1			3

Note: An empty cell denotes zero (0), i.e., that no mapping has been done to the particular concept from the particular method.

Table VII. STATISTICS OF ARCHIMATE COVERAGE, FIRST PART: BY SLOTS

Method	Business layer			Application layer			Infrastructure layer			Extensions	
	Passive structure	Behavior	Active structure	Passive structure	Behavior	Active structure	Passive structure	Behavior	Active structure	Motivation	Implementation & migration
Grundschutz	.333								.222	.444	
TRA-1	.196	.031	.227	.134		.052	.124		.175	.062	
TRITF	.302	.198	.035		.012					.430	.023
CORAS			1								
ISO/IEC 27005	.091	.106	.152	.015	.061	.076	.015	.061	.152	.227	.045
Mehari	.219	.083	.167		.01	.094		.01	.156	.25	.01
TSRMG	.161	.258	.032	.032		.032			.065	.419	
MAGERIT	.086	.043	.25	.095	.026	.095		.086	.31		.009
OCTAVE	.264	.044	.319	.011	.011	.011			.198	.132	.011
MG-3	.047	.047	.14	.047	.116	.186		.093	.186	.116	.023
NIST RMF	.137	.039	.098	.049	.108	.147	.02	.069	.245	.088	
HMG IA			.2		.2			.4		.2	
(all together)	.182	.078	.17	.045	.036	.074	.02	.037	.178	.168	.012

Note: An empty cell denotes zero (0).

ArchiMate concepts. All of the ArchiMate concepts and their respective definitions [8] used in the process of mapping are shown in table V. Relations between the concepts and further details defined by the ArchiMate modeling language (e.g., viewpoints) are not taken into account by the study.

V. RESULTS

The input items suggested by the risk assessment methods mapped to all the concepts of ArchiMate besides *plateau*, as shown in table VI. Coverage of the slots, layers and groups of

Table VIII. STATISTICS OF ARCHIMATE COVERAGE, SECOND PART. (A) COVERAGE BY LAYERS AND BY GROUPS OF CONCEPTS; (B) COUNTS OF MAPPING ITEMS, RATES OF SUCCESS AND DISPERSION IN MAPPING.

Note: In (A)*, the sum of coverage of groups including extensions equals to the sum of coverage of layers including extensions, which equals to* 1.

Method	Passive structure	Behavior	Active structure	Extensions	Business layer	Application layer	Infrastr. layer
Grundschutz	.333		.222	.444	.333		.222
TRA-1	.454	.031	.454	.062	.454	.186	.299
TRITF	.302	.209	.035	.453	.535	.012	
CORAS	1				1		
ISO/IEC 27005	.121	.227	.379	.273	.348	.152	.227
Mehari	.219	.104	.417	.260	.469	.104	.167
TSRMG	.194	.258	.129	.419	.452	.065	.065
MAGERIT	.181	.155	.655	.009	.379	.216	.397
OCTAVE	.275	.055	.527	.143	.626	.033	.198
MG-3	.093	.256	.512	.14	.233	.349	.279
NIST RMF	.206	.216	.49	.088	.275	.304	.333
HMG IA		.6	.2	.2	.2	.2	.4
(all together)	.43	.155	.235	.18	.247	.151	.422

Note: An empty cell denotes zero (0).

Method	Suggested items	Mapping hits	Security-specific items	Overly broad items	Unmapped items	Rate of success in mapping	Rate of dispersion in mapping
Grundschutz	8	9	5	1	1	.875	.125
TRA-1	53	97	1	1	1	.981	.830
TRITF	74	86		2	2	.973	.162
CORAS	8	6		3	3	.625	-0.25
ISO/IEC 27005	32	66	20	3	1	.969	1.063
Mehari	67	96		4	4	.940	.438
TSRMG	19	31		1	2	.895	.632
MAGERIT	149	116	9		15	.899	.779
OCTAVE	57	91	12	6	10	.825	.596
MG-3	19	43				1	1.263
NIST RMF	29	102	10	6		1	2.517
HMG IA	5	5		1	1	.8	
(all together)	520	748	57	28	40	.923	.438

Note: An empty cell denotes zero (0).

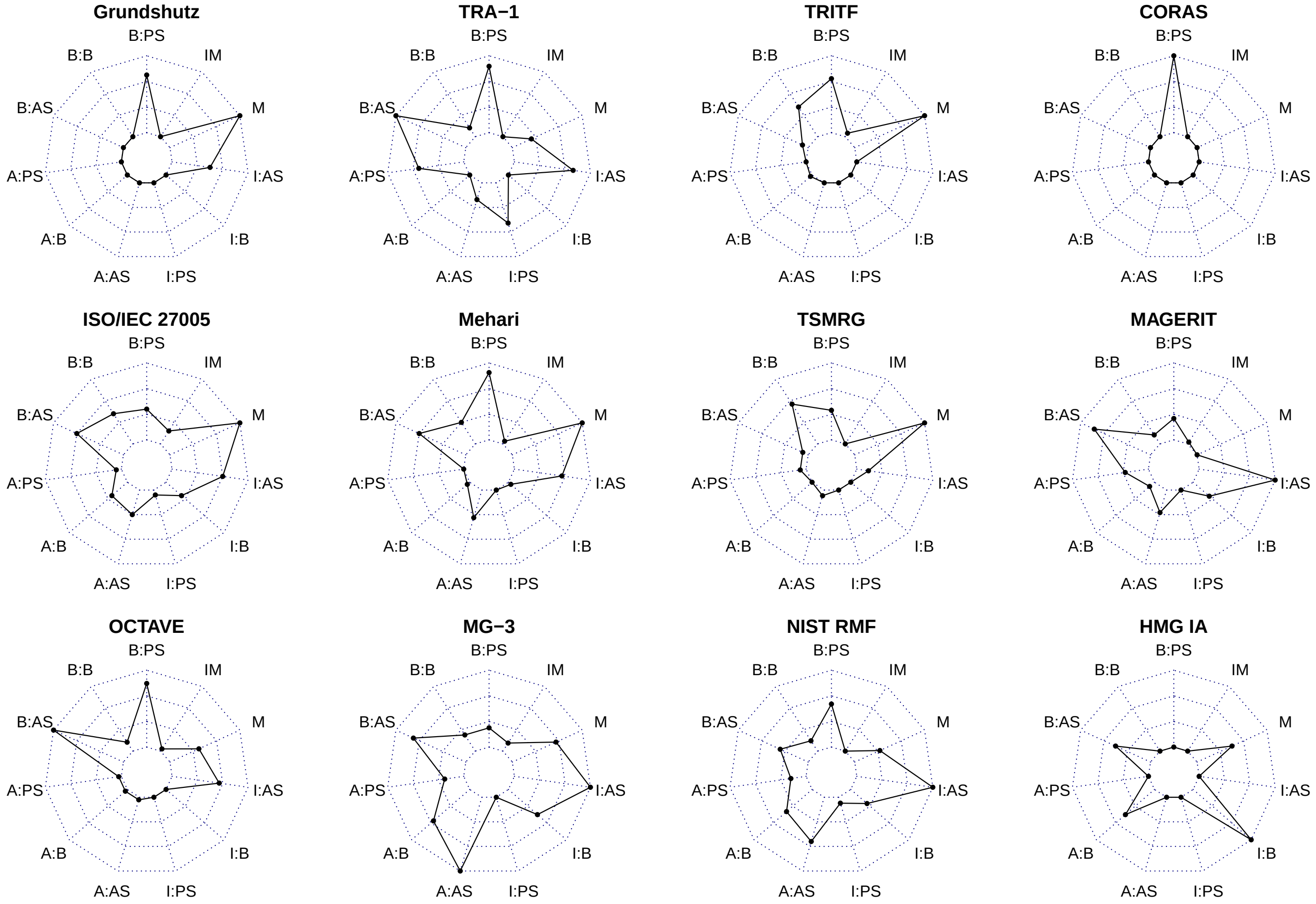

Figure 2. Relative coverage of ArchiMate slots. The names of the axes in each plot correspond to the slots of ArchiMate as in table VII, ordered counterclockwise (e.g., B:B stands for business layer and behavior, A:PS stands for application layer and passive structure, M stands for motivation extension and IM stands for implementation & migration extension). Each plot shows values from zero (the innermost level) to the maximum of values on any axis.

concepts defined by ArchiMate are shown in tables VII and VIII. Table VII shows each method's coverage of the eleven slots of ArchiMate (cf. section IV). Similarly, Fig. 2 visualizes each method's relative coverage of the slots. Table VIIIa shows each method's coverage of the layers and groups of concepts as such, including the two extensions combined. Table VIIIb

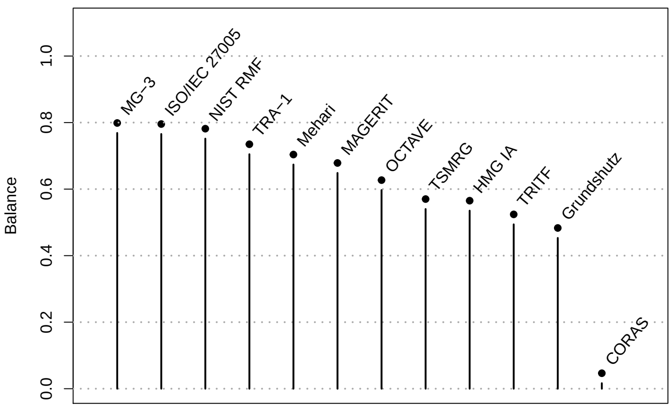

Figure 3. Balance of methods' coverage of ArchiMate slots (by suggestions of input information)

shows absolute counts of items, as well as the rates of success and dispersion in mapping.

The rate of success shows how large part of the set of the method's input terms was mapped. It is calculated as one minus the ratio of the count of unmapped items to the count of suggested items. Similarly, the rate of dispersion indicates how straight-forward the mapping was. For instance, a term mapped to multiple ArchiMate concepts increases dispersion, an unmapped term decreases dispersion, and a term mapped to precisely one ArchiMate concept influences the dispersion toward the value of 0. The rate of dispersion is calculated as the ratio of the count of mapping hits to the count of suggested items, minus one.

VI. Analysis

The input suggestions of seven out of twelve methods map to almost all slots of ArchiMate. CORAS, Grundschutz and HMG IA map to fewer (from one to four only). The results show several patterns. Majority of the methods can be rendered as centered on active structure slightly more than behavior and passive structure (i.e., data and information). Notable exceptions are CORAS, TRITF, Grundschutz and TSRMG. Motivational concepts are well covered, too, except in CORAS and MAGERIT. Among the layers of ArchiMate, business layer dominated mostly, with slight exceptions of HMG IA, NIST RMF, MAGERIT, MG-3 and MAGERIT. Implementation & migration extension as well as passive structure in the infrastructure layer (i.e., terms like signals and physical instances of data, cf. table V), received less coverage than other slots of ArchiMate.

The results show notable differences between the methods' suggestions of input information. While some methods tend to provide general suggestions (e.g., Grundschutz, CORAS, HMG IA) some others provide notably more detailed ones (e.g., MAGERIT, OCTAVE, TRA-1, MEHARI, TRITF), which also reflects on the count of different items suggested (cf. table VIIIb).

A measure of balance of each method's coverage of the eleven ArchiMate slots (data in table VII) is shown in Fig. 3. Per each method, the coverage balance is calculated based on the sum of squared errors from the theoretically most balanced coverage (i.e., all slots covered by the same amount of relative coverage), using formula 1. In the formula, $\mathbf{S}$ denotes the set of all slots of ArchiMate (cf. section IV), SC denotes a method's relative mapping coverage of a single slot (the values shown in table VII per each method), and $\overline{SC}$ denotes the mean of SC across $\mathbf{S}$ per method, which in our case always equals to $\frac{1}{11} = 0.\overline{09}$ (100% divided by the count of all slots).

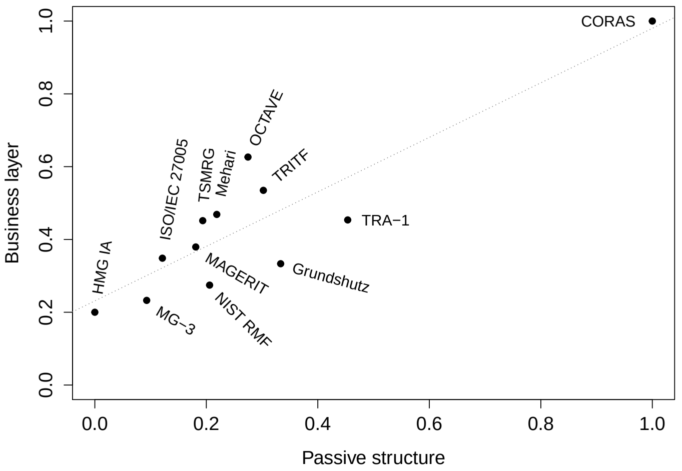

Figure 4. Scatter plot of coverage of business layer versus that of passive structure (data in table VIIIa)

Table IX. Correlations between the measures of relative coverage of layers, groups, and the two extensions (calculated using Pearson's r)

Measures	Pearson's r	p-value
Business layer vs. passive structure	.89	.0001
In passive structure: infrastructure vs. application layer	.75	.005
Infrastructure layer vs. application layer	.74	.006
Infrastructure layer vs. active structure	.72	.008
Infrastructure layer vs. business layer	-0.72	.008
Business layer vs. application layer	-0.66	.018
Behavior vs. passive structure	-0.66	.02
Application layer vs. active structure	.64	.025
Behavior in business layer vs. motivation	.6	.037

Note: Remaining measures are not listed due to low significance (p-value greater than .04).

$$\text{Balance} = 1 - \sqrt{\sum_{i \in \mathbf{S}} (\overline{SC} - SC_i)^2} \qquad (1)$$

Across all of the studied methods, a rather unexpected pattern shows: The more dominant the focus on business layer, the more prevalent the coverage of passive structure (data and information). The correlation is visible in Fig. 4, and quantified in table IX. Eigth other correlations show (cf. table IX), although less significant.

Finally, as table VIIIb shows, the total rate of success of .923 indicates that ArchiMate is capable of describing much of the input information suggested by the methods.

VII. Discussion

A. General conclusions and reflection

Our results show that among the studied methods, the sets of suggestions of input information, viewed in terms of

ArchiMate, differ to a notable extent. At the same time, most of the methods seem to strive for a broad input coverage of matters relevant to information security risk assessment, in their suggestions of input information. Furthermore, there are large differences between the quantity and detail of such suggestions. Some methods provide their users notably more concrete guidance on collecting information than others.

In a reflection, a number of factors might account for the differences in input suggestions among the methods. On the one hand, providing detailed suggestions can benefit the analysts, since identifying information that are truly relevant to a risk assessment is a difficult task deserving both considerable insight and broad thinking [1]. On the other hand, however, greatly detailed suggestions might cognitively bias the analysts toward following an established scheme that is not necessarily complete or balanced, which might lead to overlooking elements of relevance that would otherwise likely be identified. The latter might especially weigh in light of the constantly changing landscapes of technologies and threats. An alternative to choosing great detail in suggestions is to invite the analysts to themselves identify what is of most relevance for the specific target of evaluation at the day of performing the assessment (e.g., using a blank slate, top-down approach). The answer to what optimally aids achieving accurate assessment results might, however, depend on a range of attributes such as scope, detail and rigor of the assessment, disposition of the assessment process, as well as the users of the assessment method. Another candidate explanation for the choice of providing little and highly abstract suggestions might be a lack of perceived importance of suggesting in detail, e.g. based on the belief that users of the methods generally possess a comprehensive such overview. In some cases, the differences are likely influenced by different scoping of the methods. For instance, TRITF [25] sees IT risk as “business risk related to the use of IT” (p. 8), and also scores dominantly on the coverage of motivational, behavioral and passive-structural aspects of the business layer. In contrast, MG-3 [32] is intended for assessing information technology systems, compared to whole IT environments of enterprises. The scoping also reflects on the dominant coverage of application and infrastructure layers, as well as active structure across all three layers. At last, the differences between similarly scoped methods might also be explained by a lack of unification regarding what spectrum of inputs proves relevant to consider when assessing information security risk in enterprises.

Taken from a different angle, this study tested ArchiMate in terms of its semantic interoperability with the input suggestions of methods for risk assessment in information security. The study shows that although ArchiMate version 2.0 is not capable of directly describing matters that explicitly relate to information security (e.g., *vulnerabilities*, *threat profiles*, *safeguards*), it can accommodate much of the information suggested by the methods (cf. table VIIIb), i.e., information that at least indirectly relate to information security risk. While the consequence of the former might be the need to collect the explicitly security-related information using alternative means, the implication of the latter might be no less than increased ease and cost-efficiency of performing risk assessments in enterprises.

Table X. INDICATORS OF MAPPING CONSISTENCY BETWEEN REVIEWERS.

Method	Indicators (cf. table II)					
	I-1	I-2	I-3	I-4	I-5	I-6
Grundschutz	50%		50%	100%	50%	100%
TRA-1			42%	55%	8%	73%
TRITF	50%	50%	5%	56%	42%	59%
CORAS	67%			40%	67%	80%
ISO/IEC 27005	13%		22%	84%	80%	100%
Mehari		80%	12%	54%	90%	100%
TSRMG				67%	60%	83%
MAGERIT		20%	38%	75%	80%	79%
OCTAVE		5%	9%	30%	72%	42%
MG-3			26%	39%		72%
NIST RMF	8%		38%	50%	67%	58%
HMG IA	50%			50%	100%	50%

Note: An empty cell denotes zero (0%).

B. Validity

Due to the choice of a non-security-centric conceptual framework (ArchiMate), as well as the necessity of human processing of data and interpretation of meaning, several threats to reliability and validity of the study exist. First, it can be argued that ArchiMate is not suitable for measuring and comparing attributes of the sets of input information suggested by methods for information security risk assessment. While admitted on the one hand, to the knowledge of the authors there are no established frameworks that would provide a more balanced and resoluted structure for comparing the different enterprise and IT-related terms to date, on the other hand. Moreover, it is not intended to infer anything about the methods' accuracy nor other performance qualities based on the methods' input coverage of ArchiMate. The picture can, however, aid an enterprise in choosing a suitable risk assessment method with regards to an existing documentation of enterprise architecture (EA), or vice versa, in tailoring a suitable approach to documenting EA to provide adequate support for a given risk assessment method. Second, the process of selecting methods was to some extent driven by a qualitative collective judgment rather than a purely formal model. The differences between individual inclusion suggestions were however small and discussions smooth. Third, the process of data extraction was perceived as a cognitively demanding task, prone to leaving out desirable data. To lessen the risk, each method was reviewed and extracted data from independently by two researchers. Fourth, mapping the input information items to the concepts of ArchiMate (data synthesis) was the most challenging part, especially with regards to reliability, seen as the probability of arriving at the same results through independently repeated such runs of review and data extraction. Indicators of mapping consistency between the two reviewers for each method described below and presented in table X, reflect a degree of uncertainty of the individual mapping results. Such inconsistencies in the individual mapping were however addressed by subsequent group reviews and mapping corrections, as described in section III.

Table X shows values of the indicators of mapping consistency defined in table II. Higher values mean more consistency in mapping in the pairs of reviewers. As the values show, the mapping consistency was less than optimal. On the other hand however, a lack of consistency in mapping of each item led to a consensus-based decision between the two reviewers, before the final mapping was made.

C. Summary and outlook

Despite inherent challenges, the study attempts to provide an adequate picture of what types of input information do the different risk assessment methods suggest, and the extent to which the sets of the suggestions are unified among the studied methods. Moreover, the results show that although not entirely, the enterprise architecture modeling language ArchiMate is capable of aiding the use of information security risk assessments through supplying input information suggested by the risk assessment methods, to a fair extent. Given the wide use of ArchiMate, EA documentation in its format might be a promising source of guidance for performing risk assessments, as well as a way of making the process of information security risk assessment more efficient.

In the future, both more unification among the individual risk assessment methods' suggestions of input information, and a higher semantic interoperability between them and EA models such as those based on ArchiMate, could be beneficial. To the latter end, Grandry et al. [16] proposed a security risk management extension to ArchiMate. Although the extension defines a set of concepts commonly used in information security risk management (e.g., risk, impact, event, threat, vulnerability, risk treatment, control, etc.), there remains a potential to further improve mapping between the terms used by the studied risk assessment methods (cf. table I), through introducing additional concepts. While the concepts proposed by [16] enable modeling of the results (output) of a risk assessment, they do not enable modeling of information needed or beneficial as input to the risk assessment. Based on the security-specific input terms encountered in this study, a few suggestions of the latter kind, together with instance-level examples, could be: *risk factor* as an external factor influencing risk (e.g., unreliable electrical distribution); *protection scope* as a delimitation of a control's protective capability (e.g., cryptographic verification of integrity of transferred data within a single session); *performance metric* as a means to quantify security-effectiveness (e.g., comparison of intrusion protection system logs versus all observed incidents); *protection zone* as a physical/geographical or logical zone with a degree of control over the environment (e.g., premises of a building with doors and locks); *security class* signifying a level or set of security requirements/constraints related to an element or asset and its usage (e.g., internal/confidential/secret); *technological basis* potentially implying a specific set of vulnerabilities (e.g., RSA cryptographic algorithm, or wireless networking based on IEEE 802.11n); *external dependency* as a dependency on something, the availability or presence of which is effectively out of control for an organization (e.g., availability of a cellular network, or confidentiality of data stored using a cloud storage operated by a different organization); *security profile* as a generic profile describing common or typical threats/vulnerablities related to a technological basis (e.g., vulnerability profile for wireless network communications).

Acknowledgment

This study has been financed by the Swedish Armed Forces and SweGrids, the *Swedish Centre for Smart Grids and Energy Storage* (www.swegrids.se); thereunder Fortum and the Swedish Energy Agency.

References

[1] A. Jones and D. Ashenden, *Risk Management for Computer Security: Protecting Your Network & Information Assets*. Elsevier Butterworth-Heinemann, 2005.

[2] W. Stallings and L. Brown, *Computer Security. Principles and Practice*, 2nd ed. Harlow, UK: Pearson, 2012.

[3] S. H. Von Solms and R. Von Solms, *Information Security Governance*. Springer, 2009.

[4] ENISA. (2014) Inventory of Risk Management / Risk Assessment Methods. [Online]. Available: http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html

[5] F. Macedo, "Models for assessing information security risk," Master's thesis, Instituto Superior Técnico, Universidade Técnica de Lisboa, Oct. 2009. [Online]. Available: https://fenix.tecnico.ulisboa.pt/downloadFile/2589867718508/dissertacao.pdf

[6] L. Skyttner, *General systems theory: problems, perspectives, practice*, 2nd ed. World Scientific, 2005.

[7] M. Lankhorst, *Enterprise architecture at work: Modelling, communication and analysis*. Springer, 2013.

[8] The Open Group, "ArchiMate 2.0 Specification, Technical Standard," Reading, UK: The Open Group, 2012. [Online]. Available: http://www.opengroup.org/archimate/

[9] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (isra)," *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45–52, 2013.

[10] ENISA. (2007) Methodology for evaluating usage and comparison of risk assessment and risk management items. [Online]. Available: http://www.enisa.europa.eu/publications/archive/methodology-for-evaluating-usage-and-comparison-of-risk-assessment-and-risk-management-items/at_download/fullReport

[11] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide," in *Availability, Reliability and Security, 2009. ARES'09. International Conference on*. IEEE, 2009, pp. 726–731.

[12] S. Fenz and A. Ekelhart, "Verification, validation, and evaluation in information security risk management," *Security & Privacy, IEEE*, vol. 9, no. 2, pp. 58–65, 2011.

[13] G. Giannopoulos, R. Filippini, and M. Schimmer. (2012) Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. Ispra (VA), Italy. [Online]. Available: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf

[14] E. Johansson, "Assessment of Enterprise Information Security – How to make it Credible and efficient," Ph.D. dissertation, KTH Royal Institute of Technology, Stockholm, Sweden, Oct. 2005. [Online]. Available: http://kth.diva-portal.org/smash/get/diva2:14379/FULLTEXT01

[15] T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *Systems Journal, IEEE*, vol. 7, no. 3, pp. 363–373, Sept 2013.

[16] E. Grandry, C. Feltus, and E. Dubois, "Conceptual integration of enterprise architecture management and security risk management," in *Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2013 17th IEEE International*. IEEE, 2013, pp. 114–123.

[17] P. Szwed and P. Skrzyński, "A new lightweight method for security risk assessment based on fuzzy cognitive maps," *International Journal of Applied Mathematics and Computer Science*, vol. 24, no. 1, pp. 213–225, 2014.

[18] Central Communication and Telecommunication Agency. (2013) CRAMM (web site). [Online]. Available: http://www.cramm.com/

[19] COUNTERACT consortium. (2006) COUNTERACT: Cluster of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities. [Online]. Available: http://trainingsecurity.uitp-events-expo.org/sites/default/files/pdf/COUNTERACT%20Guidelines_lr.pdf

[20] Agence nationale de la sécurité des systèmes d'information. (2013) EBIOS 2010 - Expression of Needs and Identification of Security Objectives. [Online]. Available: http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html

[21] The Open Group. (2013) The Open Group FAIR Certification Program. [Online]. Available: http://www.opengroup.org/certifications/openfair

[22] Risk Management Insight. (2007) An introduction to factor analysis of information risk. [Online]. Available: http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf

[23] Bundesamt für Sicherheit in der Informationstechnik, "Bsi-standard 100-3 risk analysis based on it-grundschutz," Bonn, Germany, 2008.

[24] Communications Security Establishment and Royal Canadian Mounted Police, "Harmonized Threat and Risk Assessment (TRA) Methodology," Canada: Communications Security Establishment, 2007.

[25] ISACA, "The Risk IT Framework," Rolling Meadows, USA: ISACA, 2009.

[26] M. S. Lund, B. Solhaug, and K. Stølen, *Model-driven risk analysis: the CORAS approach.* Springer, 2011.

[27] ISO/IEC, "International Standard ISO/IEC 27005," Switzerland: ISO/IEC, 2011.

[28] Club de la Sécurité de l'Information Français, "MEHARI 2010 Processing guide for risk analysis and management," Paris: Club de la Sécurité de l'Information Français, 2011.

[29] Microsoft Corporation, "The Security Risk Management Guide," San Francisco, USA: Microsoft Corporation, 2006.

[30] Ministerio de Administraciones Públicas, "MAGERIT – version 2: Methodology for Information Systems Risk Analysis and Management: Book I – The Method," Madrid, Spain: Ministerio de Administraciones Públicas, 2006. [Online]. Available: https://www.ccn-cert.cni.es/publico/herramientas/pilar44/en/magerit/meth-en-v11.pdf

[31] Carnegie Mellon University, "OCTAVE Method Implementation Guide v2.0," USA: Carnegie Mellon University, Oct. 2001, doi:10.1093/jmp/jhs081.

[32] Communications Security Establishment, "A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems," Ottawa, Canada: Government of Canada, 1996.

[33] NIST, "NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments," Gaithersburg, USA: NIST, 2012.

[34] National Technical Authority for Information Assurance, "HMG IA Standard No. 1 Technical Risk assessment," Cheltenham, United Kingdom: National Technical Authority for Information Assurance, 2009.

[35] The Open Group. (2009) TOGAF version 9. [Online]. Available: http://pubs.opengroup.org/architecture/togaf9-doc/arch/

[36] BiZZdesign. (2012) Enterprise Architecture with TOGAF® 9.1 and ArchiMate® 2.0. White paper. [Online]. Available: http://www.bizzdesign.com/assets/Downloads/Whitepaper-ArchiMate-2-TOGAF-9.1-Version-2.pdf

[37] B. Scholtz, A. Calitz, and A. Connolley, "An analysis of the adoption and usage of enterprise architecture," in *Enterprise Systems Conference (ES), 2013.* IEEE, 2013, pp. 1–9.