Final Causal Explanations

Document information	
Project Title	EMFASE
Project Number	E.02.32
Project Manager	University of Trento
Deliverable Name	Final Causal Explanations
Deliverable ID	D3.2
Edition	00.01.00
Template Version	03.00.00
Task contributors	
Deep Blue; University of Trento; SINTEF; University of Southampton	

Please complete the advanced properties of the document

Abstract

The objective of EMFASE WP3 is to provide causal explanations of the phenomena observed in the empirical evaluations. The purpose of such explanations is to provide a better understanding of the underlying mechanisms of (the application of) risk assessment methods and thus to support the development of risk assessment method selection guidelines. In this deliverable we present the final theories of causal explanation. The theories are based on existing theories, but they have been specialized for security risk assessment methods based on the results of the empirical studies conducted in the project.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
Federica Paci / UoS	WP3 Leader	07/02/2016

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
Rainer Koelle / SJU	WP-E Officer	14/03/2016

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
Fabio Massacci (UNITN)	Coordinator/Professor	11/03/2016

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	DD/MM/YYYY	Working Document	F. Paci (UoS)	ToC
00.00.02	29/02/2016	Working Document	F. Paci (UoS)	Draft of Section 3 and 4
00.00.03	07/03/2016	Working Document	F. Paci (UoS)	Draft of Section 2
00.00.03	08/03/2016	Working Document	K. Labunets (UNITN)	Draft of Section 2
00.00.03	08/03/2016	Working Document	F. Paci (UoS)	Executive Summary and Introduction
00.00.04	10/03/2016	Final Document	F. Paci (UoS)	Revised Section 4 and Added Section 5
00.00.05	11/03/2016	Final Document	E. Chiarani, F. Massacci (UNITN)	Quality Check and approval
00.01.00	14/03/2016	Final Document	R. Koelle	Final Review

Intellectual Property Rights (foreground)

This deliverable consists of foreground owned by one or several Members or their Affiliates.

Table of Contents

List of tables

List of figures

Executive summary

The objective of EMFASE WP3 is to provide causal explanations of the phenomena observed in the empirical studies. The purpose of such explanations is to provide a better understanding of the underlying mechanisms of (the application of) risk assessment methods and thus to support the development of risk assessment method selection guidelines. The causal explanations will be built upon existing theories, but they will be specialized for security risk assessment methods and refined based on the empirical results of the project.

This document provides final theories for explaining and exploring the mechanisms of security risk assessment. In addition, the document shows how the theories are applied to the results of the experiments conducted within EMFASE.

More specifically, this document makes the following contributions.

- A theory that explains how features of catalogues determine the actual and perceived efficacy of a security risk assessment
- A revised version of cognitive fit theory [1] that explains the difference in performance of tabular and graphical risk models
- An explanation of the results of the experiments conducted within EMFASE based on the above theories
- A discussion of the implications of the results on security risk assessment practices.

1 Introduction

1.1 Purpose of the document

The objective of EMFASE WP3 is to provide causal explanations of the phenomena observed in the empirical studies. The purpose of such explanations is to provide a better understanding of the underlying mechanisms of (the application of) risk assessment methods and thus to support the development of risk assessment method selection guidelines.

This document provides the final version of the theories for explaining and exploring the mechanisms underlying a security risk assessment process. The document introduces a theory on how catalogues' features affect the actual and perceived efficacy of a security risk assessment process. In addition, the document introduces a slightly different version of cognitive fit theory [1] adapted to explain the results on comprehensibility of risk models.

The document is structured as follows. In Section 2, we summarize the main results obtained from the experiments on comparing the actual and perceived efficacy of textual and visual methods for security risk assessment, the effect of using catalogues when conducting a security risk assessment, and the comprehensibility of risk models. In Section 3, we present a theory that describes how different features of catalogues contribute to an effective risk assessment process when performed by non-security experts and a slightly modified version of cognitive fit theory. In Section 4, we discuss how the proposed theories explain our experimental results. In Section 5, we conclude the document by highlighting the implication of our results for current practices in security risk assessment.

1.2 Intended readership

D3.2 is mainly an internal working document for EMFASE. Thus, intended readers of this document are primarily the EMFASE project partners and the EUROCONTROL. This document is to be used by the members of the project EMFASE as it provides final theories of causal explanation for the results of the empirical studies conducted within EMFASE.

Other potential readers are generally all stakeholders within the ATM domain that need to take security into account in an operational area. More specifically, the document is of interest to all SESAR JU projects within the transversal areas of WP16 that are related to security management and risk assessment. For these stakeholders the document gives insight into some of ATM security risk assessment methods that could be relevant to apply or investigate further.

1.3 Inputs from other projects

The document does not make use of input from other projects, but the content is related to both SESAR 16.02.03 and SESAR 16.06.02. References to these projects are given in the relevant sections.

1.4 Acronyms and Terminology

Term	Definition
ATM	Air Traffic Management
E-ATMS	European Air Traffic Management System
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency.

Term	Definition
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
TAM	Technology Acceptance Model
MEM	Method Evaluation Model
PEOU	Perceived Ease to Use
PU	Perceived Usefulness
ITU	Intention to Use
Actual Efficacy	Actual efficacy is the degree to which a method achieves its objectives (Actual Effectiveness) and is free of effort (Actual Efficiency).
Perceived Efficacy	Perceived efficacy is the degree to which person believes that a method achieves its intended objectives (Perceived Usefulness) and using it is free of effort (Perceived Ease of Use).

2 Summary for Results

This section summarizes the results from the experiments comparing textual versus visual security risk assessment methods, the experiments on the effect of using catalogues during a risk assessment process, and the experiments on comparing the comprehensibility of textual versus visual security risk modelling notations. In the remainder of the section, we will use the term “novices” to denote subjects who participated in our experiments who have no expertise in the application domain and in security (e.g MSc students). We will call domain-experts, the subjects who have only expertise in the application domain (e.g ATM professionals), while we will name security experts, the subjects who have expertise in security.

2.1 Textual vs Visual methods for security risk assessment

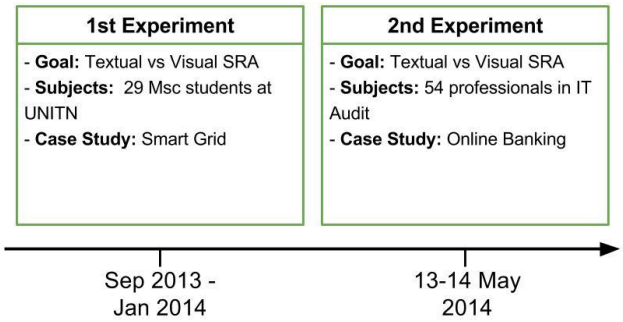

Figure 1. EMFASE Experiments: Textual vs Visual SRA Methods

We conducted two experiments with MSc students and professional to assess the actual and perceived efficacy of textual and visual methods for security risk assessment. The results are consistent across the two experiments [6]. *Actual efficacy* is the pragmatic success of the method, i.e. the extent to which it improves the performance of the task in question. *Perceived Efficacy*, instead, is the degree to which a person believes that using a particular method would be free of effort and it will be effective in achieving its intended objectives.

Actual efficacy. There is no statistically significant difference in the actual efficacy of textual and visual methods for security risk assessment.

Perceived efficacy. The perceived efficacy of visual security risk assessment methods is higher than the one of textual methods.

2.2 The effect of using catalogues of threats and security controls

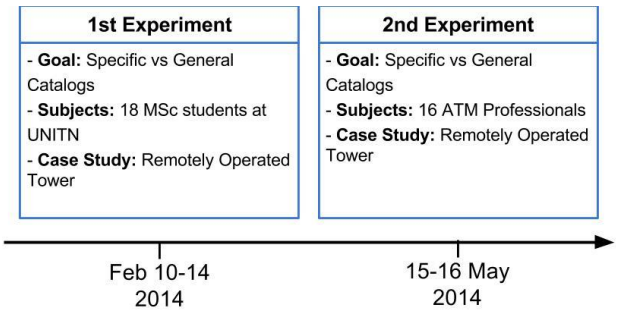

Figure 2. EMFASE Experiments: The effect of using catalogues

We have conducted two experiments on the effect of using catalogues of threats and security controls on the actual and perceived efficacy of a security risk assessment process [7,8]. The first experiment involved 18 MSc students who have limited knowledge in security and in the application domain, the Remotely Operated Tower (novices). In the second experiment, instead we had 15 ATM professionals as participants. 10 participants had knowledge in the ATM domain but not in security (domain experts) while the remaining participants had knowledge in the ATM domain and in security (security experts).

Actual efficacy. Novices produced threats and security controls of slightly higher quality with domain-specific catalogues rather than with general-domain catalogues. The domain experts who did not have expertise in security also produced threats and security controls of higher quality with domain-specific catalogues. Moreover, the quality of threats and controls produced by domain-experts with domain-specific catalogues is higher than the one produced by security experts without catalogues. However, both results are not statistically significant due to the small sample size.

Perceived efficacy. The domain-specific catalogues were perceived to be more useful than the domain-general catalogues by novices with statistical significance. While domain experts have the same perceived efficacy of the domain-specific catalogues and domain-general catalogues but this result is not statistically significant due to the small sample size.

2.3 Comprehensibility of risk modelling notations

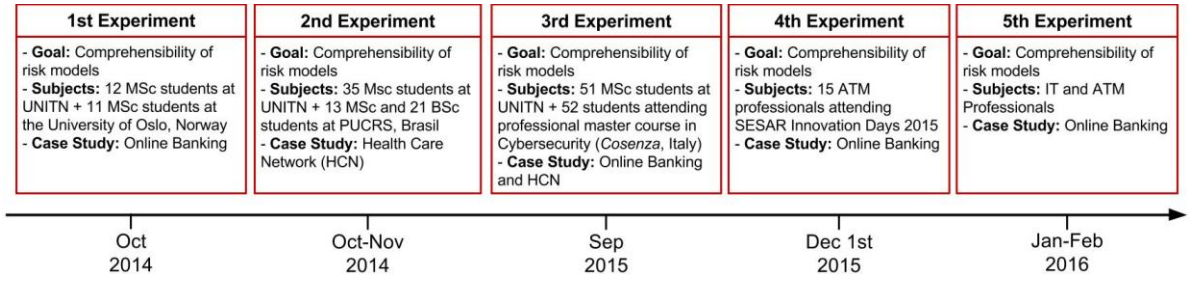

Figure 3. EMFASE Experiments: Comprehensibility of risk models

We run a series of 5 experiments to investigate the comprehensibility of tabular and graphical risk modeling notations. The comprehensibility has been measured in terms of precision and recall of the answers given to comprehension questions, which are classified in simple and complex questions.
Precision represents the correctness of the answers given to a question, and recall is the completeness of the answers given to a question. The results consistent across all the experiments are that tabular risk model has higher actual comprehension than the graphical one. Subjects who used the tabular risk model gave more precise and complete answers to the comprehension questions. Moreover, the results showed that tabular risk models have higher comprehension than the graphical ones with respect to simple comprehension task and slightly higher comprehension for complex comprehension task.

3 Theories of Causal Explanations

In this section we first report the theory that explains the results of the experiments on the use of catalogues, and then the theory that motivates the results on the comprehensibility of visual and textual notations for risk assessment.

3.1 A Theory for Catalogue Effectiveness

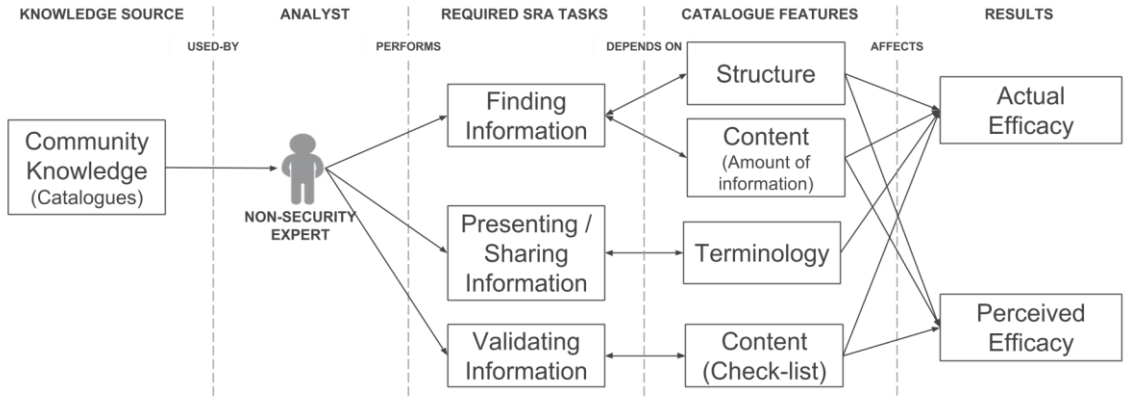

Figure 4. A Theory of Catalogue Effectiveness

We present a theory on how different features of catalogues contribute to an effective risk assessment process when performed by non-security experts. Figure 4 illustrates the key elements of the theory and their relationships. Additional details are provided in [7,8].

The model first explains the core tasks to perform a security risk assessment and the features of catalogues needed for these tasks. At the end, the theory models the relationships between the tasks conducted in a security risk assessment, the catalogues features and the actual and perceived efficacy of a security risk assessment process.

3.1.1 Concepts

Non-security experts will mainly *use* community knowledge in the form of catalogues to conduct a security risk assessment. Community knowledge [4] is "personal knowledge" shared between members, for example, in a documented form (catalogue being just one of such form). Personal knowledge is tacit knowledge that people create by themselves or learn from their own experience.

Non-security experts will mainly *perform* the following core tasks during a security risk assessment:

- **Finding information** implies identification of assets, threats and security controls,
- **Presenting/sharing information** focuses on documenting results to other stakeholders using a terminology appropriate to the domain.
- **Validating information** requires checking that the assets, threats and security controls identified by the analyst are complete and comply with security standards and regulations.

The execution of the above tasks *depends on* specific features of catalogs. Key features of a catalogue are:

- **Catalogue Structure.** The way threats and security controls are presented and linked together.

- **Catalogue Content.** The number and type of threats/ security controls contained in the catalogs.
- **Terminology**. Standard language to define security threats and controls.

These catalogues features ultimately affect the *actual efficacy* and *perceived efficacy* [3] of a security risk assessment process.

3.1.2 Relationships

The catalogue structure may affect both actual and perceived efficacy of finding information. If the structure of a catalogue is not clear and logical it will increase the effort required to non-security experts to find threats and security controls.
The catalogue content (amount of information) may affect both actual and perceived efficacy of finding information. Non-security experts can struggle with too big catalogues because they do not know how to start a risk assessment if they have too many options. Hence, amount of information presented in a catalogue can affect both actual and perceived efficacy of a security assessment.
The catalogue content (checklist) may affect both actual and perceive efficacy of validating information. The catalogues may be useful when analysts need to check that no threats or security controls were overlooked. The completeness of the results has a positive effect on the actual and perceived efficacy of the risk assessment process.
Terminology may affect actual efficacy of sharing and presenting information. Catalogue can support non-security experts with standard terminology accepted in both the domain and the security field. Even users without solid background both in either domain or security can produce results understandable by experts. The clear and uniform presentation of the results improves the actual efficacy of a security risk assessment.

Based on the above theory, when non-security experts use catalogues with a) clear and logic structure, b) reasonable size and good coverage of threats and security controls and c) specific terminology for the application domain, finding information, sharing information and validating information will be more efficient and effective and therefore, the actual and perceived efficacy of a security risk assessment process will be enhanced.

3.2 Cognitive Fit Theory Applied to Risk Modelling Notations

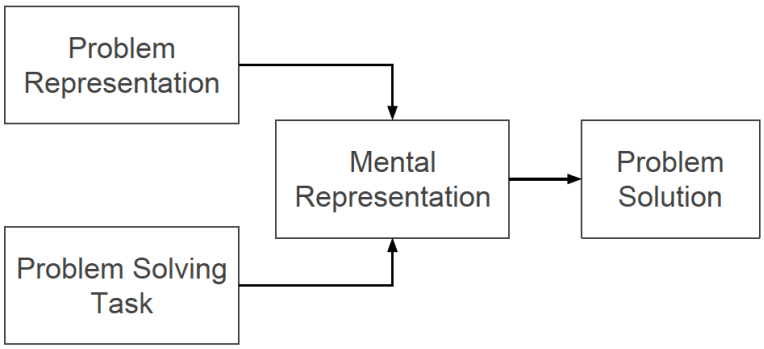

Figure 5. Cognitive Fit Theory

To explain the results on comprehensibility of risk assessment notations we resort on the cognitive fit theory [1]. The cognitive fit theory (see Figure 5) states that performance of a task will be enhanced when there is a cognitive fit (a match) between the information emphasized in the representation type

and that required by the task type. Problem solving with cognitive fit results in increased problem solving efficiency and effectiveness.

The cognitive fit theory has been applied to explain the differences in performance with graphical and tabular notations when used in decision-making processes.

Graphical and tabular notations may contain the same information, but they represent that information in fundamentally different ways; graphical notations emphasize spatial information while tabular notations emphasizes symbolic information. Spatial information captures relationships among data, while symbolic information encode specific data values.

Therefore, according to cognitive fit theory, graphical representations will facilitate spatial tasks that require to make associations or perceiving relationships in the data; while tabular notations will facilitate symbolic tasks that extract or act on discrete data values.

This theory would then predict that graphical risk notations are easier to comprehend given their capacity for capturing spatial relationships. Tabular risk notation would be better only when actual computations ought to be performed such as computing the likelihood or severity of an attack.

However, we argue that tables also capture linear spatial relationships. In tabular risk models the name of the column identifies the type of a risk element (e.g., assets, threats, vulnerabilities, impact, likelihood, and security controls) and each row relates elements to each other. Hence, we can consider the proximity of cells along a row or along a column as a simple spatial relationship.

Therefore, the efficiency and effectiveness of a task that emphasizes both spatial and symbolic information should be higher when using tabular risk models.

4 Discussion

In this section we discuss how the results of our experiments can be explained by the theories presented in the previous section.

4.1 Textual vs Visual methods for security risk assessment

In our studies [6], visual and textual risk assessment methods showed similar actual efficacy, while the perceived efficacy of the visual method is always higher.

The results on actual efficacy can be explained by cognitive fit theory: for the methods that we evaluated in our studies, there is a match between the information provided by the risk modeling notation and the information required by the task that analysts have to perform during a risk assessment process.

Regarding perceived efficacy, the results can also being explained by the theory on perceived efficacy that we proposed in D3.1. The theory reports the key features of a security risk assessment method that have an effect on methods' perceived efficacy. The higher perceived efficacy for the visual method can be explained by the fact that the visual method has a *clear process* supporting main steps of security risk assessment process and a *visual representation* of risk model, which provides the "big picture" and therefore makes easier for analysts to summarize the results of a security risk assessment process.

4.2 Effect of using catalogues of threats and controls

Catalogue's Features	**Domain-specific catalogues**	**Domain-general catalogues**
Catalogue Structure	Clear and Logical (link between threats and security controls)	Complex (Link between threats and security controls in a separate section)
Catalogue Content	32 threats and 51 security controls	621 threats and 1444 security controls
Terminology	ATM Specific Security Terminology	Common Security Terminology

Table 1. Catalogues Features

Our studies [7,8] show that the use of catalogues can mitigate a lack of security expertise and provide a good starting point for the analyst. The domain experts who had no knowledge in security have identified with domain-specific catalogues threats and security controls of higher quality of domain and security experts without catalogues. This result can be explained based on the theory that we have introduced in Section 3.1, which links the features of catalogues, the core tasks of a risk assessment process and the actual and perceived efficacy of a security risk assessment process.

In our study, the domain-specific catalogues have clear and simple structure (32 threats divided into three topics with links to security controls), reasonable size (155 pages), support users with ATM specific threats and security controls, and related ATM specific terminology. In contrast, domain-general catalogues have complex structure (links between threats and controls in a separate section), big size and coverage (621 threats and 1444 security controls in 6 topics), supports users with common security terminology, and cover a wide range of IT security problems and solutions.

Therefore, the higher actual efficacy of the results obtained by domain-experts without security expertise are due to the fact that the features of the domain-specific catalogues facilitated the core tasks of a security risk assessment: identifying threats and security controls, sharing threats and security controls, and validating identified threats and security controls. In particular:

- *Finding information* (threats and security controls) was easier with domain-specific catalogues because of their clear and logical structure and the reasonable *size and coverage* of specific threats and security controls for the ATM domain. In fact, domain-experts reported that "*I read only the titles [namely the reference to the "Generic Threat" and the "Attack Threat"], they were quite explanatory, therefore a very short consultation of the catalogue allowed me to produce enough content*" and "*Once identified the threat, finding out controls was really a mechanical work*".
- *Sharing and discussing* the identified threats and security controls was also made easier by the ATM specific terminology contained in the domain-specific catalogues. As suggested by participants, "*The catalogue could be seen as a useful tool, able to formalize the controls that have been formulated in an informal way, and to lead them back into a common nomenclature*".
- Similarly, *validating the identified threats and security controls* was made easier by the *content of the catalogues*, which has been used as checklist for missing threats or security controls. Indeed, the participants claimed that: "*The first step is to use your own experience and then to use the catalogue to cover generic aspects that could be forgotten*".

4.3 Comprehensibility of risk modelling notations

The results show that, overall, the tabular risk model provides a higher actual comprehension than the graphical one. Subjects who applied the tabular risk model gave more precise and complete answers to the comprehension questions. Regarding complexity of comprehension questions, the precision of answers was higher with the tabular risk model for simple comprehension questions, while the precision of tabular and graphical risk models was similar for complex questions. Recall was always higher with the tabular risk model for simple and complex questions.

These results can be explained by the revised cognitive fit theory introduced in section 3.2. The comprehension tasks/questions in our study are a mix of symbolic and spatial task. They require first the subjects to identify a specific element (symbolic task) and then to identify other elements in relationship with the first one (spatial task). The location of the specific risk element is easier with tabular risk models because the name of the column identifies the type of a risk element (e.g assets, threats, vulnerabilities, impact, likelihood, and security controls). Similarly, the proximity of cells along a row can be considered as a simple spatial relationship, therefore facilitating the identification of risk elements in relationship to each other. In contrast, locating and searching is less immediate in graphical risk models because in these models the risk elements are identified by means of graphical icons that first must be learned by the subjects to locate these elements.

We can therefore conclude that the comprehensibility of tabular risk models is higher because there is a match between the information emphasized by tabular risk models and the comprehension task. Tabular risk models emphasize both symbolic and spatial information, which is both required by the comprehension task. See [9] for more details.

5 Conclusions

A key result of our studies [5,6,7,8,9] is that domain-experts without security expertise using domain-specific catalogues of threats and security controls achieve better results than domain-experts with security expertise. These results are explained by our theory on catalogues effectiveness which argues that when non-security experts use catalogues with a) clear and logic structure, b) reasonable size and good coverage of threats and security controls and c) specific terminology for the application domain, finding, sharing and validating threats and security controls will be more efficient and effective and therefore, the actual and perceived efficacy of a security risk assessment process will be higher.

This result may have interesting implications on security risk assessment practices. To facilitate analysts during a security risk assessment process, the method should support catalogues usage from the first steps. Usually, an SRA process requires identifying three main components: 1) assets that should be protected, 2) threats that can harm identified assets, and 3) security controls that can mitigate identified threats. Catalogues can provide an ample source of knowledge for all three components. The analysts just need to limit scope to the assets, which are relevant to the system, and in this respect domain knowledge is all that is needed. Consequently, using catalogues even domain experts without security expertise can identify a set of preliminary threats and security controls. Thus, catalogues facilitate a prima facie SRA by domain expert. From a company's perspective domain experts are easier to find internally than security experts who are expensive to get.

Another key result that may have implications for security risk assessment practices is that tabular risk model lead to better efficiency and effectiveness if the task to be performed requires to search or locate specific risk elements and to make associations among risk elements. Given that the core tasks in a security risk assessments require to identify risk elements and link them together, using a security risk assessment method which uses tabular risk model would have higher efficiency and effectiveness.

6 References

[1] Iris Vessey. Cognitive fit: A theory-based analysis of the graphs versus tables literature. *Decision Sciences*, 22(2):219–240, 1991.

[2] Robert E Wood. Task complexity: Definition of the construct. *Organizational Behavior and Human Decision Processes*, 37(1):60–82, 1986.

[3] Daniel L. Moody. The method evaluation model: A theoretical model for vali- dating information systems design methods. In *Proceedings of the 11th European Conference of Information Systems*, pages 1327–1336, 2003.

[4] Lynne M Markus. Toward a theory of knowledge reuse: Types of knowledge reuse situations and factors in reuse success. *Journal of Management Information Systems*, 18(1):57–93, 2001.

[5] Katsiaryna Labunets, Federica Paci, Fabio Massacci, Martina Ragosta, and Bjørnar Solhaug. A First Empirical Evaluation Framework for Security Risk Assessment Methods in the ATM Domain. In *Proceedings of the 4th SESAR Innovation Days*. SESAR, 2014.

[6] Katsiaryna Labunets, Federica Paci, Fabio Massacci, and Raminder Ruprai. An experiment on comparing textual vs. visual industrial methods for security risk assessment. In *Proceedings of the 4th IEEE International Workshop on Empirical Requirements Engineering at the 22nd IEEE International Requirements Engineering Conference*, pages 28–35. IEEE, 2014.

[7] Martina de Gramatica, Katsiaryna Labunets, Fabio Massacci, Federica Paci, and Alessandra Tedeschi. The Role of Catalogues of Threats and Security Controls in Security Risk Assessment: An Empirical Study with ATM Professionals. In *Proceedings of the 21st International Working Conference on Requirements Engineering: Foundation for Software Quality*, volume 9013 of Lecture Notes in Computer Science, pages 98–114. Springer, 2015.

[8] Katsiaryna Labunets, Federica Paci, and Fabio Massacci. Which Security Catalogue Is Better for Novices? In *Proceedings of the 5th IEEE International Workshop on Empirical Requirements Engineering at the 23rd IEEE International Requirements Engineering Conference*, pages 25–32, 2015.

[9] Katsiaryna Labunets, Yan Li, Fabio Massacci, Federica Paci, Martina Ragosta, Bjørnar Solhaug, Ketil Stølen, Alessandra Tedeschi. Preliminary Experiments on the Relative Comprehensibility of Tabular and Graphical Risk Models. In the *Proceedings of 5th SESAR Innovation Days*. SESAR, 2015.