Selection of Risk Assessment Methods Object of Study

Document information	
Project Title	Empirical Framework for Security Design and Economic Tradeoff – EMFASE
Project Number	E.02.32
Project Manager	University of Trento
Deliverable Name	Selection of Risk Assessment Methods Object of Study
Deliverable ID	D1.1
Edition	00.01.03
Template Version	03.00.00
Task contributors	
SINTEF; University of Trento; Deep Blue.	

Abstract

The main objective of EMFASE WP1 is to develop a framework for empirical evaluation of methods for ATM security risk assessment. This document presents the methods we select as objects of the empirical studies, the identified selection criteria, as well as how we identified the selection criteria. The deliverable moreover presents a general overview of the state of the art regarding methods for security risk assessment, as well as the main findings from interviews and surveys among relevant ATM professionals regarding their needs and expectations from such methods.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
Bjørnar Solhaug, SINTEF	WP1 leader	28/02/2014
Federica Paci, UNITN	Project member	27/02/2014
Fabio Massacci, UNITN	Project coordinator	14/02/2014
Katsyarina Labunets, UNITN	Project member	14/02/2014
Martina De Gramatica, UNITN	Project member	14/02/2014

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
Elisa Chiarani, UNITN	Project manager assistant	24/02/2014
Federica Paci, UNITN	Project member	27/02/2015
Federica Paci, UNITN	Project member	08/04/2014
Elisa Chiarani, UNITN	Project manager assistant	09/04/2014

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
Rainer Koelle, EUROCONTROL	Project Officer	14/03/2014

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
Fabio Massacci, UNITN	Project coordinator	09/09/2014

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	14/01/2014	Document structure	B. Solhaug	Document creation
00.00.02	06/02/2014	Draft	F. Massacci, K. Labunets, M. De Gramatica	Data gathering and analysis
00.00.03	14/02/2014	Draft	B. Solhaug, F. Paci	Full first draft of all main sections
00.00.10	20/02/2014	First version	B. Solhaug	First version of deliverable
00.00.11	24/02/2014	Working	E. Chiarani	Quality check completed; minor changes

00.00.12	27/02/2014	Working	F. Paci	Internal review
00.00.13	28/02/2014	Working	B. Solhaug	Revision after internal review and quality check
00.01.00	28/02/2014	Review ready	B. Solhaug	Prepared for external review
00.01.01	27/03/2014	For approval	B. Solhaug	Revision after external review
00.01.02	08/04/2014	Internal Review	F. Paci	Minor remarks
00.01.03	09/04/2014	Quality check	E. Chiarani, F. Massacci	Quality check and approval

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 main objective of WP1 of the EMASE project is to develop a framework for empirical evaluation of methods for security risk assessment for the ATM domain. The framework shall provide means for categorizing security risk assessment methods, and provide general principles for evaluating and comparing such methods.

The purpose of this deliverable is to document the security risk assessment methods that will be the main objects of the empirical studies and the evaluation within the EMFASE project. While our framework for empirical evaluation should be applicable to any security risk assessment method that is adequate for the ATM domain, it is of course infeasible to study all existing methods in the course of this project. The deliverable gives an overview of the state of the art, and describes our initial scheme for classifying security risk assessment methods based on the needs of ATM stakeholders. Subsequently we describe in more details the methods that will be applied in our empirical studies, and the reason for this selection.

The needs of the ATM stakeholders were identified via surveys and interviews of ATM professionals that to a greater or lesser extent are required to conduct security risk assessments. The gathered data was analyzed by qualitative research techniques to identify the most important criteria that should be fulfilled by methods for security risk assessment. The identified criteria were clear process, specific controls, easy to use, coverage of results, tool support and comparability of results. Based on these criteria, the meaning of which are explained in the deliverable, we identified a set of further parameters for classifying risk assessment methods, where each parameter correspond to a method feature or property that may contribute to fulfill one or more of the criteria identified by the professionals.

Using the criteria and parameters we identified six criteria for the selection of the specific risk assessment methods that will serve as our main objects of study. The selection criteria are 1) relevance for the ATM domain, 2) readiness for (empirical) study, 3) in-house expertise (within the EMFASE consortium), 4) coverage of the identified criteria and parameters, 5) self-contained methods, and 6) complementarity of selected methods.

Finally, the deliverable presents in more details the selected methods, namely SecRAM, CORAS and the EUROCONTRL ATM Security Risk Management Toolkit, as well as the reason for this selection. In the course of the EMFASE project, we may select further security risk assessment methods to study, but this depends on how the project evolves and which further needs we may identify while developing the EMFASE empirical framework.

1 Introduction

1.1 Purpose of the document

The main objective of WP1 of the EMFASE project is to develop a framework for empirical evaluation of methods for security risk assessment for the Air Traffic Management (ATM) domain. The framework shall provide means for categorizing security risk assessment methods, and provide general principles for evaluating and comparing such methods.

The purpose of this deliverable is to document the security risk assessment methods that will be the main objects of the empirical studies and the evaluation within the EMFASE project. While our framework for empirical evaluation should be applicable to any security risk assessment method that is adequate for the ATM domain, it is of course infeasible to study all existing methods in the course of this project. In this deliverable we give an overview of the state of the art, and we describe our initial scheme for classifying security risk assessment methods based on the needs of ATM stakeholders. Subsequently we describe in more details the methods that will be applied in our empirical studies, and the reason for this selection.

More specifically, the document is structured as follows. After the overview of the state of the art in Section 2, we describe in Section 3 how we gathered from relevant ATM professionals the underlying data for classifying methods for security risk assessment. In Section 4 we present our classification, which is based on the criteria derived from the gathered data, as well as further relevant classification parameters that we identified. The section also relates the criteria and parameters, and indicates the main means for their verification. In Section 5 we present the criteria for the selection of our method objects of study, and in Section 6 we describe in more details the specific methods we selected. Section 7 gives a brief overview of relevant support material for the selected methods, before we conclude in Section 8.

1.2 Intended readership

The intended readers of this document 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 for 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 the main criteria that should be fulfilled by methods for ATM security risk assessment, and also which methods that could be relevant to apply or investigate further.

1.3 Inputs from other projects

This deliverable uses in particular inputs from SESAR project 16.02.03 Security Risk Assessment – Security Risk Assessment Methodology, since this methodology is one of those considered by EMFASE for serving as object to empirical studies and evaluation. Project 16.02.05 Harmonized ATM Security Best Practices also provides relevant input, in particular the Minimum Set of Security Controls (MSSC).

1.4 Glossary of terms

Term	Definition
Asset	Anything that has value to the organization
Consequence	Impact
Impact	Adverse change to the level of business objectives achieved
Information asset	Knowledge or data that has value to the organization

Term	Definition
Information security	Preservation of confidentiality, integrity and availability of information
Likelihood	The probability or frequency of occurrence
Risk	The combination of the likelihood of an unwanted incident and its consequence
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Threat	Potential cause of an unwanted incident
Treatment	Measure to modify risk
Unwanted incident	Event that harms an asset
Vulnerability	Weakness of an asset or control that can be exploited by a threat

1.5 Acronyms and Terminology

Term	Definition
ATM	Air Traffic Management
E-ATMS	European Air Traffic Management System
RA	Risk assessment
RAM	Risk assessment method
SecRAM	SESAR Security Risk Assessment Method
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.
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.

2 State of the Art

In this section we give a general overview of established standards, methods and best practices for security risk management of information systems.

Most methods for risk management and risk assessment follow (to greater or lesser extent) the process defined by the ISO 31000 standard [9]. The purpose of the standard is to provide principles and guidelines for risk management independent of domains and the kinds of risk that are addressed (such as safety, environment, security, finance, etc.). The proposed risk management process consists of seven activities. Five of these include risk assessment, which should be conducted at a regular basis. These five activities are context establishment, risk identification, risk analysis, risk evaluation, and risk treatment. The remaining two activities are continuous and comprise communication and consultation, as well as monitoring and review.

The ISO/IEC 27005 standard [13] complies with ISO 31000, but is tailored for information security risk management. The notion of information security is defined by the ISO/IEC 27001 information security standard [12] as the preservation of confidentiality, integrity and availability of information. Other relevant properties that can be involved are authenticity, accountability, non-repudiation and reliability. The two standards include guidelines, and come with lists of controls, threats and vulnerabilities that should be considered. The NIST SP 800-30 [20] is a standard for risk management for IT systems developed by the US National Institute of Standards and Technology. It provides a terminology for IT risk management and specifies a process for how to conduct risk assessment, and is supported by a catalogue of recommended security controls [21].

There are a number of national level standards and guidelines for risk management that are closely related to these international standards. The UK standard on technical risk assessment [22] is issued by the Cabinet Office, and shall be applied to government IT systems to support the identification and estimation of security risks, and the selection of appropriate controls for risk mitigation. Other similar examples are the French EBIOS [1], the Spanish MAGERIT [19] and the German IT-Grundschutz [4].

In addition to international and national standards there are a number of approaches from industry, like COBIT [14], CRAMM [27], the Microsoft Security Risk Management Guide [18], and SABSA [24]. COBIT and SABSA focus on business goals/requirements and the protection or fulfillment of these by means of security controls. CRAMM was originally developed for the British governmental agency CCTA in the eighties, and is now in its version 5. It follows a process similar to ISO/IEC 27005, and supports organizations to achieve ISO/IEC 27001 certification. The Microsoft guide defines a risk management process of four phases that shall aid stakeholders in proactively identifying and mitigating IT security risks.

Available methods that have been developed by academia and research institutes include OCTAVE [2], SQUARE [16], SREP [17] and CORAS [15]. OCTAVE is a risk-based strategic assessment and planning method for security conducted over three phases. The method is asset-driven, so the first phase is dedicated to the identification of critical assets, as well as threat profiles. The subsequent phases are for vulnerability mitigation, and for risk identification and mitigation, respectively. SQUARE has a wider scope than risk assessment alone, as it aims to elicit security and privacy requirements. Risk assessment is conducted as one of the phases of the process, and is applied to support the requirements elicitation. SREP supports a similar process to identify and analyze security requirements, and is compliant with several standards, including ISO/IEC 27001 and the Common Criteria [11]. CORAS is a model-driven approach to risk assessment that is closely based on the ISO 31000 standard. It comes with practical guidelines and techniques to support the different activities, as well as language and tool support for the necessary risk modeling.

Risk assessment is a critical part of aviation and ATM, but traditionally the focus has been on safety, as exemplified by the EUROCONTROL ESARR 4 [6] requirements to risk assessment and mitigation in ATM. However, the need for security management steadily increases due to the criticality of ATM information systems and services. Guidance such as the Manual for National ATM Security Oversight [7] and the ATM Security Risk Management Toolkit [5] highlight the need for security risk assessment in ATM. Moreover, the SESAR JU has projects dedicated to the development of methods for security risk assessment of ATM systems. In particular, the SESAR ATM Security Risk Assessment Method (SecRAM) [26] shall aid SESAR Operational Focus Areas (OFAs) in assessing and documenting security risks. SecRAM is compatible with ISO/IEC 27005 and is defined over a process of seven steps, ranging from asset identification to risk treatment. The method is asset driven, and the focus is on information assets and services with the aim of protecting their confidentiality, integrity and availability. The SecRAM Implementation Guidance Material [25] provides guidelines for how to apply the method in practice.

Standards and guidelines such as the ISO/IEC risk management standards mainly describe the underlying terminology, the processes to implement, and the activities that are required to be conducted. How to do risk assessment in practice and which techniques to use are often explained to a much lesser extent. Such techniques can be for threat identification and modeling, likelihood and consequence estimation, risk evaluation, etc. We will not give a detailed overview of such techniques here as they are numerous and of many different kinds. The reader is referred to the IEC 31010 guidance [10] that gives a comprehensive overview. Some well-known techniques for threat modeling are Misuse Cases [29], Attack Trees [28] and Microsoft Threat Modeling [30]. The notations facilitate the identification and analysis of threats and the attacks these threats can initiate. Risk and threat modeling not only facilitates conducting the risk assessment, but also the documentation of the results. Many approaches, such as SecRAM, uses table formats for the documentation.

The purpose of this overview of the state of the art is to provide a brief outline of the relevant background to this deliverable and to the tasks of EMFASE WP1. The work package develops a scheme for classification and comparison of methods for security risk assessment, as well as means and criteria for evaluating such methods. In the following sections we present our initial set of criteria and parameters for method classification. These will be elaborated during the course of the project, but at this stage they serve as a basis for our selection of the risk assessment methods object of study. The evaluation and comparison of the state of the art is outside the scope of this deliverable; instead, the main purpose is to select the objects of study by considering the state of the art and the overall objectives of WP1.

3 Data Gathering Process

In order to enable an empirical evaluation and comparison of methods for security risk assessment we need to identify the criteria with respect to which the methods shall be evaluated. Because EMFASE targets the ATM domain in particular we did an initial survey among ATM stakeholders to elicit such criteria. The survey included a questionnaire that was filled in by the participants individually, as well as group interviews where the participants were organized into separate focus groups of 5-6 people in each group.

The participants were all professionals from different organizations and enterprises within the aviation domain. While their background in security and risk management are of varying degree, they are all to some extent required to consider security risks and their mitigation as part of their work. The participants were hence a representative selection of ATM stakeholders with qualified opinions about and insights into the methodic needs for conducting a security risk assessment.

The questionnaire included an open question about the main success criteria for security risk assessment methods, and this topic was also covered by the interviews. We analyzed the questionnaire answers and the interview transcripts using *coding* [3], which is a content analysis technique from grounded theory. The qualitative analysis was conducted as follows.

1. We analyzed the responses to the open question and the interview transcripts to identify the recurrent patterns (codes) about the success criteria for the security risk assessment methods.
2. The identified codes were grouped by their similarity and classified into categories.
3. For each category we counted the number of statements as a measure of their relative importance.

Table 1 summarizes the main criteria reported by the professionals. We considered as the main identified criteria only the ones for which at least ten statements were made by the participants. Each of the criteria is explained in the next section, but we can observe here that while the main bulk of the statements fall into six main categories, the total share of other statements is significant (approx. 45%). This indicates some spread in the opinions of the ATM stakeholders, and that we may need to elaborate and refine the criteria during the course of the project.

Criterion	**Number of statements**
Clear process	28
Specific controls	24
Easy to use	19
Coverage of results	14
Tool support	13
Comparability of results	10
Other	88
Total	**196**

Table 1 – Occurrences of reported success criteria

4 Method Classification

There are of course many different parameters and aspects that can be considered for the classification of methods for security risk assessment. For one thing, considering the overview of the state of the art in Section 2, what is understood by a risk assessment method can to some extent vary. At the very least, a method should consist of a well-defined procedure or process for attaining an objective. While this is the case for all of the considered risk assessment methods, there is much variation regarding further support. Such support may include practical guidelines, assessment techniques, repositories and tools. By risk assessment technique we mean a practical means for accomplishing a particular task during the process, such as the estimation of the risk likelihoods. While some methods are quite self-contained in the sense that they come with techniques and/or tool support, other leave it to the method user to select which existing, available techniques to use.

In our classification and evaluation of security risk assessment methods we will take into account all additional support that comes with each method. SecRAM, for example, comes with repositories of assets and controls, while CORAS comes with a tool for risk modeling.

The classification scheme is based on the data gathered from the ATM professionals. Guided by the criteria that we identified from these data, we have identified further method features or artifacts that could contribute to fulfill the criteria. The classification is the initial scheme for supporting the method evaluation in EMFASE; in the continuation of the project we will revise it based on any new insight, knowledge or further basis for extracting relevant criteria.

4.1 Identified Criteria

In the following we explain in more detail the six criteria we identified based on the qualitative analysis using coding. Note that the criteria are not necessarily orthogonal, since, for example, ease of use may depend on other criteria like clarity of process and tool support. Also note that the selected quotations are slightly paraphrased.

The qualitative content analysis using coding requires a classification of the codes (statements) that in turns gives a measure of their relative importance. This classification is part of the analysis, and therefore obviously not given in advance. After the explanation of each criterion we give some example statements to illustrate how the statements were categorized.

Clear process. The main criterion reported by the ATM professionals (14% of the statements) is that a security risk assessment method should have a clear process. This means that the method should come with a process of well-defined steps, and each step should be supported by guidelines for how to conduct it.

Some of the statements related to this category are as follows.

- *The method should be explicit about the objective of each task, the input to the task, how to conduct it and which output it shall produce.*
- *There should be logical steps to follow throughout the assessment process.*
- *A method is not good if it does not provide concrete and practical guidelines, including what to do, which information to gather and how to document it.*

Specific controls. The second criterion (12% of the statements) is that the method should aid the identification of security controls (means for risk mitigation) that reduce the risks to an acceptable level. The controls must be specific to the organization and problem context (i.e. the target and the objectives of the assessment).

Some of the statements related to this category are as follows.

- *The countermeasures identified by the security risk assessment method must be accustomed to the context.*
- *The method should aid in improving the security in comparison with the current situation, i.e. the situation before conducting the security risk assessment.*
- *The method must target the problem at hand and suite the organization.*

Easy to use. The third criterion (10% of the statements) is that the security risk assessment method should be easy to use. This means that the method comes with a process that is simple, easy to understand and follow, free from redundant steps, and that it helps in finding an agreement with the relevant stakeholders.

The following are some of the relevant statements made by the professionals.

- *The method should not elaborate things too much.*
- *The risk assessment should be easy to handle and understand, and it should be possible to conduct it within a reasonable amount of time.*
- *The risk assessment method should be applicable with simplicity, and the users should be able to achieve the results by simple actions.*
- *The method must be applicable, straightforward, simple, logical and fast.*

Coverage of results. The fourth reported criterion (7% of the statements) is coverage or completeness of the results. This means that the method shall help to find all significant security risks within the defined target of analysis.

The relevant statements include the following.

- *The method should help finding the most complete set of risks related to security.*
- *The coverage of the method is important. This includes the identification of risks, the identification of means for mitigation (preventive, detective and reactive), the coverage of the threat space, and the coverage of the full life cycle of the system under threat.*

Tool support. The fifth criterion (6% of the statements) was related to the importance of having tool support for the method.

The following are example of statements related to this criterion:

- *The method should come with tool support for the automated calculation of risk levels.*
- *Tool support should be provided to enable the consideration of several thousand factors (like threats, threat scenarios, assets and asset support).*
- *Tools that implement the method should be provided.*
- *For cases with numerous threats, there are also lots of duplications that make the assessment difficult. A tool that implements the method would be helpful.*
- *Tools for automating steps of the method should be provided.*

Comparability of results. The sixths of the most reported criteria (5% of the statements) was related to the ability to compare security risk assessment results. This means that the method should be easily repeatable, and that the results can be compared to both previous and other assessments.

Some of the statements of the professionals related to this criterion include the following:

- *The results of applying the method should be comparable with previous results.*
- *The method should be repeatable, measurable and comparable.*

4.2 Further Classification Parameters

Based on the criteria we identified using the data provided by the ATM professionals, we have identified further support or method features and artifacts that are relevant. These are parameters for security risk assessment classification that can contribute to fulfill one or more of the six main criteria identified by the professionals. This is an initial set of parameters that is likely to be extended and/or revised during the course of the EMFASE project. At this point we did the parameter identification by considering typical features of security risk assessment methods, and selecting those that can be related to the criteria identified by the professionals.

Compliance with ISO/IEC standards. Compliance with established international standards is a demand by many organizations. Although compliance should not be an absolute criterion for selecting a suitable method for security risk assessment, it is relevant for many stakeholders and decision makers regarding risk and security management. The most obvious standards to consider for our purposes are the ISO 31000 standard on risk management and the ISO/IEC 27005 standard on information security risk management.

Well-defined terminology. Understanding, communicating, assessing and documenting security risks require a precise and commonly understood vocabulary. It is therefore important that any method for security risk assessment provides the terminology that is needed in order to use the method, to describe the relevant elements and the relations between them, to communicate the results to other stakeholders, etc. The terminology should also be reflected by any documentation templates or modeling techniques that should support the method.

Documentation templates. Templates or other means for documenting the assessment results can be of good help, not only for the documentation itself, but also as guidance on what information to gather, how to gather it, and how to capture the relations between results. Such relations can, for example, be between an asset, a threat that may harm it, and the vulnerability that may be exploited by the threat.

Modeling support. Risk and threat modeling can serve as very useful techniques for conducting the risk assessment. The modeling language should reflect the underlying terminology and provide structure and guidance for how to do the steps or tasks of the method. Modeling can moreover serve as a means for documentation of the risk assessment results.

Practical guidelines. This parameter is strongly related to the criteria of process clarity and method ease of use. Such guidelines should be precise descriptions about how to conduct each step of the method, which techniques to use, who should be involved, which information to gather, etc. This parameter may be relevant to take into account as some methods provide little or no guidance on how to do a risk assessment, but rather focus on what the assessment should cover. This is in particular the case for the mentioned ISO/IEC standards.

Assessment techniques. Risk assessment involves the core risk management activities of risk identification, risk analysis and risk evaluation [9]. For the practitioners it is not enough to know only what the assessment involves, but also how to do it. Assessment techniques are more specific than practical guidelines and can, for example, be qualitative or quantitative means for likelihood estimation, consequence estimation, risk evaluation, cost estimation, etc. A comprehensive overview and classification of risk assessment techniques are provided in the ISO 31010 standard [10].

Lists and repositories. Supporting lists and repositories include lists of assets, threats, vulnerabilities and treatments/controls. Examples of such lists are those provided by the ISO/IEC 27005 standard.

4.3 Criteria and Supporting Parameters

In Table 2 we give an overview of the relations between the identified criteria and parameters for the classification of the security risk assessment methods. The six criteria are listed horizontally, while the related criteria and parameters are listed vertically. A marked cell indicates that the supporting criterion/parameter may contribute to the fulfillment of the criterion in question. For example, a clear process could make the method easy to use and also facilitate the comparison of results. Moreover, available documentation templates could help clarifying the process, make the method easy to use and facilitate comparison. Note that we did not include compliance with standards in this matrix since this is not a supporting feature in the sense that the other parameters are.

	Supporting criteria						Supporting parameters					
Criterion	Clear process	Specific controls	Easy to use	Coverage of results	Tool support	Comparability of results	Well-defined terminology	Documentation templates	Modeling support	Practical guidelines	Assessment techniques	Repositories
Clear process							X	X	X	X	X	
Specific controls												X
Easy to use	X				X		X	X	X	X	X	X
Coverage of results										X		X
Tool support												
Comparability of results	X			X			X	X	X	X	X	X

Table 2 – Supporting criteria and parameters

4.4 Means for Verification

In the studies of methods for security risk assessment there are certain criteria and parameters that need to be investigated empirically through their application in realistic settings. However, for some of the criteria and parameters it may suffice to do a simple check of what is offered by the method. In Table 3 we have indicated for each criterion/parameter whether its fulfilment in some cases can be verified by a check (C) or if a more thorough empirical (E) investigation is required.

Notice, importantly, that while some of the criteria and supporting parameters can be verified by a simple check, they may still need to be investigated further in the empirical evaluation of the criteria. Hence, a tick in the C column does not exclude it from empirical evaluation. For example, while it can be easily checked whether tool support is provided, there is still a need to investigate to what extent the tool actually aids the practitioners and facilitates the security risk assessment, as well as the extent to which the tool itself is practical and easy to use. The same is the case for, for example, documentation templates and modeling support, where an evaluation of the extent to which they are fit for their purposes may be required.

The purpose of Table 3 is therefore not to conclude on how we need to go by for evaluating security risk assessment methods with respect to the identified criteria. It is rather an initial indication which features and properties that we in particular need to consider in the development of our empirical evaluation framework.

Evaluation criterion/parameter	C	E
Clear process		X
Specific controls		X

Easy to use		X
Coverage of results		X
Tool support	X	
Comparability of results		X
Well-defined terminology	X	
Documentation templates	X	
Modeling support	X	
Practical guidelines	X	
Assessment techniques	X	
Repositories	X	
Compliance with ISO/IEC	X	

Table 3 – Means to verify the fulfillment of the identified criteria and parameters

5 Selection Criteria

As mentioned in the introduction, it is infeasible within the course of the EMFASE to do in-depth empirical studies of all relevant methods for security risk assessment. Instead we will select a few methods that will serve as the EMFASE empirical method's object of study. In the following we describe the main criteria we have used for making our selection.

Relevance for the ATM domain. EMFASE targets the needs of the aviation domain and ATM professionals regarding security risk management of ATM systems. An obvious criterion for the selection of methods to study is therefore that they are relevant for and applicable to the ATM domain.

Readiness for study. By this criterion we mean that the methods we select should be readily applicable to ATM use case scenarios. That is to say, we should be able to set up our studies by relatively little preparations from our side and from other case study participants. Such preparations typically include ensuring our own expertise in using the methods, as well as any needed training of other participants.

In-house expertise. This criterion is related to the previous one, and means that we (to the extent possible) select methods for which there is already in-house expertise within the EMFASE project. This is to ensure that we can provide the necessary and adequate training of the participants using the methods, and that we can do qualified monitoring of the correct application of the methods.

Coverage of identified criteria and parameters. By this criterion we mean that the selected methods should as much as possible cover the success criteria and supporting parameters described in Section 4. While this selection criterion can be checked *a priori* for the supporting parameters, this is of course not the case for the success criteria that are what we aim to investigate and achieve *a posteriori* understanding of. However, our selected methods are those we believe are suitable for investigating all of the success criteria to understand how they can be fulfilled.

Self-contained. By a self-contained method for security risk assessment, we mean that it comes with all the techniques, guidelines, documentation means, etc. that are needed in order to conduct the complete assessment according to the method.

Complementarity. By this selection criterion we mean that the selected methods in combination should (as much as possible) cover the criteria identified by the ATM professionals, thereby covering the research questions we seek to investigate using our empirical framework.

6 Selected Methods

In this section we describe in more detail the methods that we have selected to serve as our benchmark methods for the empirical studies. While the EMFASE project will evaluate only this selection of existing methods, the concepts, terminology, study design and metrics, etc. that we develop to do this evaluation will be of a general nature. That is to say, our empirical evaluation framework shall be generally applicable so as to enable later replications and comparable studies using alternative methods for security risk assessment.

In this initial phase of the EMFASE project we have selected three risk assessment methods, namely SecRAM [26], CORAS [15] and the EUROCONTROL ATM Security Risk Management Toolkit [5]. During the course of the project we may include further methods, depending on our empirical findings and further research needs.

As explained in the following, the reason for this selection is by reference to the selection criteria described in the previous section.

Relevance for the ATM domain. SecRAM the EUROCONTROL toolkit were developed for ATM security risk assessment, so the relevance of these methods is self-evident. CORAS was developed to support risk assessment in general and has no specific support for ATM. However, CORAS is applicable also to this domain, and it supports both the ISO/IEC 27005 and ISO 31000 standards which are important bases for SecRAM and the EUROCONTROL toolkit, respectively.

Readiness for study. This is clearly fulfilled by the three selected methods. They are all applicable to the domain, they come with the necessary support to conduct complete risk assessments, and EMFASE has personnel with strong familiarity with all of the methods.

In-house expertise. This is also clearly fulfilled since SINTEF was the developer of CORAS, and because SINTEF (via NATMIG) was one of the contributors to the development of SecRAM and the SecRAM guidance material. Personnel from UNITN have undergone a tutorial on the EUROCONTROL toolkit, and also applied it in case studies.

Coverage of identified criteria and parameters. Each method covers several of the identified supporting parameters, and in combination they cover all of them. All of them also come with features that provide the basis for investigating all of the main success criteria identified by the ATM professionals.

Self-contained. No security risk assessment method is completely self-contained in the sense that it provides the means for tackling any issue that may arise. However, the selected methods have been designed with the aim of supporting the analysts as much as possible throughout the whole risk assessment process. The differences between the methods, such as modeling vs. tables for documentation, gives us a good basis for investigating which features are useful and for what purposes.

Complementarity. Considering our identified success criteria and supporting parameters, the methods in combination give a good coverage of the topics we seek to investigate. The obvious differences between the methods moreover give a good basis for identifying strengths and weaknesses, and which of the method features that are adequate and useful for ATM professionals. For example, one of the main differences between SecRAM and CORAS is that while the former was developed to support personnel with little or no security expertise and relying on repositories, the latter was developed to support risk analysts in analyzing any system (possibly) from scratch.

The three methods were briefly described in the state of the art overview of Section 2. In the following we present them in more detail before making a brief comparison of the three.

6.1 SecRAM

The SESAR ATM Security Risk Assessment Method (SecRAM) [26] is developed within the SESAR JU project 16.02.03 (Security Risk Assessment – Security Risk Assessment Methodology). This is a so-called transversal project as the developed artifacts shall be applied across all other SESAR projects. The objective is to provide a method that is applicable to all Operational Focus Areas, that is understandable to personnel with little expertise and background in security and risk management, and that allows security risk assessment results from different OFAs to be compared.

Compared to most of the risk assessment methods described in Section 2, SecRAM is rather light weight. However, users of the method are supported by various repositories such as a security register (with lists of assets, threats, threat scenarios, vulnerabilities and controls), security high level documents (including the Minimum Set of Security Controls (MSSC) and security policies), and the Operational Service and Environment Description (OSED). These repositories, along with the SecRAM Implementation Guidance Material [25], compensates the relative simplicity of the method by providing much of the risk information that otherwise would have to be built from scratch.

Figure 1 gives an overview of the SecRAM process. It starts with the asset identification, and the subsequent identification and evaluation of risks are with respect to these assets. The final risk treatment shall identify options for mitigating unacceptable risks. This overall process is divided into seven steps as follows.

Step 1: Primary asset identification and impact assessment. Primary assets are of two kinds, namely service assets and information assets. Service assets are, for examples, those the loss or degradation of which make it impossible to carry out the business mission of the OFA. Information assets include information that is required for carrying out the business mission and information that is of strategic or confidential nature. For each primary asset, the required level of confidentiality, integrity and availability (CIA) must be specified. This denotes the level of criticality on a scale ranging from 1 (N/A) to 5 (catastrophic). This impact assessment is done with respect to seven different impact areas (e.g. personnel and capacity), and indicates the potential harm to the assets.

Step 2: Supporting asset identification and valuation. Supporting assets are those possessing the vulnerabilities that are exploitable by threats aiming to impair primary assets. They are of various kinds, including hardware, software, personnel, networks and storage media. All supporting assets within the scope of the assessment must be identified, and each primary asset must be linked to at least one supporting asset. Supporting assets inherit the CIA levels of the primary assets they support.

Step 3: Threat scenario identification. The objective of this step is to identify potential threat scenarios for the OFA in question. A threat scenario is the combination of a threat, a vulnerability and a primary asset. A threat is an attacker with its resources, objectives and goals, whereas a vulnerability is a weakness of a supporting asset. After the identification of the threat scenarios, each resulting combination of a threat and primary asset is assessed by indicating the CIA properties that may be harmed.

Step 4: Impact evaluation. Step 4-6 of SecRAM are conducted to do the risk evaluation. The impact evaluation is an assessment of the potential harm of each threat, which typically equals the highest impact that was identified during the threat scenario identification.

Step 5: Likelihood evaluation. The likelihood evaluation is an estimation of the chance for a threat to carry out an attack as described by the threat scenarios. SecRAM uses a likelihood scale of five levels ranging from 1 (very unlikely) to 5 (certain).

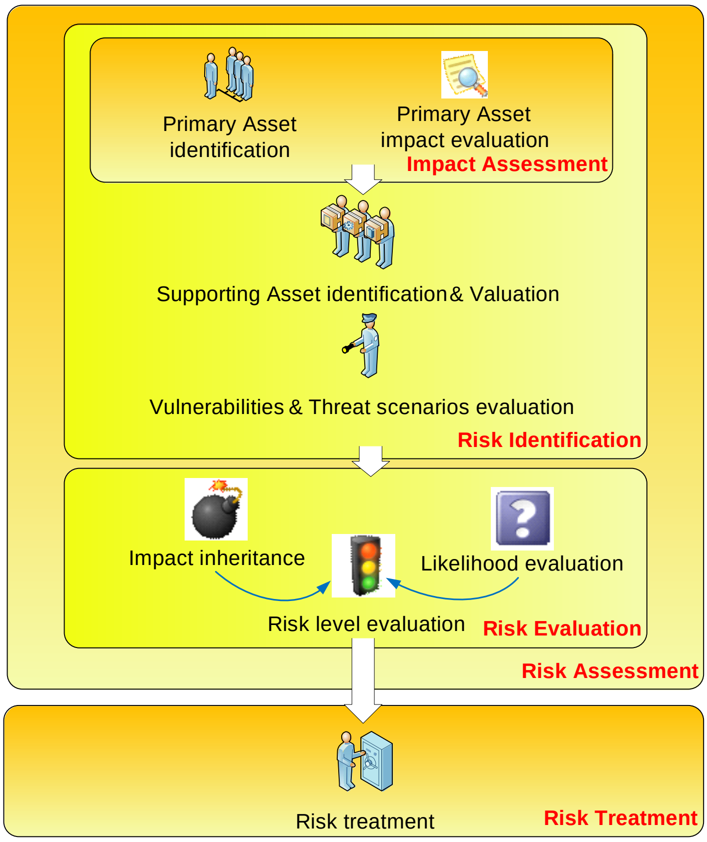

Figure 1: SecRAM process overview

Step 6: Risk level evaluation. For the risk level evaluation SecRAM uses a 5x5 risk matrix combining the five levels of impact and likelihood. The matrix defines three risk levels, namely low, medium and high. Each of the identified threats is evaluated according to its evaluated impact and likelihood.

Step 7: Risk treatment. This step involves the identification of options for risk mitigation. The options are of the following kinds: Accept (tolerate), reduce (treat), avoid and transfer. The reduce option involves the identification of controls that will reduce impact and/or likelihood. The avoid options means to terminate the activity that causes the risk, whereas transfer is to handle the responsibility of the risk in question to another party.

In addition to the available repositories and supporting material such as the implementation guidance material, SecRAM comes with table templates for conducting and documenting all steps of the method.

6.2 CORAS

CORAS [15] is a model-driven approach to risk assessment that is closely based on the ISO 31000 risk management standard. It consists of three tightly interwoven artifacts, namely the CORAS method, the CORAS language and the CORAS tool. The method follows a process of eight steps that complies with the risk assessment process of the ISO standard. In addition to describing the steps and the activities to be conducted, CORAS comes with practical guidelines and techniques that are needed for carrying out the risk assessment. The language is a graphical notation with various kinds of diagrams that are used throughout the process from beginning to end. While being a formal language with support rigorous analysis of the diagrams, the language was developed to facilitate communication between stakeholders involved in the assessment, including people with little technical background. The CORAS tool is basically a diagram editor for creating all kinds of CORAS diagrams. The tool was designed to facilitate on-the-fly modeling of diagrams during structured brainstorming.

The CORAS method is asset-driven. This means that the assets that are the focus of the risk assessment are identified and documented during the initial phase of the process. All subsequent tasks of risk and threat identification are with respect to these assets only, which is to ensure that the risk assessment focuses on the objectives of the assessment.

The four first steps of the CORAS method correspond to the first step of the context establishment of the ISO standard (cf. Section 2). The remaining four steps correspond to the remaining four steps of the standard. In the following description of the CORAS method we align the steps with the standard in order to highlight the compliance. We also describe the modeling support for each step.

Step 1-4: Context establishment using asset diagrams. The context establishment includes setting the scope and focus of the assessment, describing and documenting the target of analysis, identifying and documenting the assets, setting the (qualitative of quantitative) scales for likelihoods and consequences, and defining the risk evaluation criteria. The target of analysis should be described as precisely as possible, at the desired level of abstraction and details, using a suitable modeling language such as the UML [23]. The subsequent risk identification is conducted by systematically going through the target models. The models therefore need to contain all relevant information such as users, roles and actors, components, services, network, work and business processes, etc. The assets are documented using CORAS *asset diagrams*. These diagrams show not only the assets with respect to which risks are to be identified, but also who is the party (stakeholder) and how the assets are related. The party is the entity that assigns value to the assets, and therefore the stakeholder for whom the risk assessment is done.

Step 5: Risk identification using threat diagrams. The risk identification is conducted by an analysis team that includes, in addition to the risk analysts, a group of people with different expert insight into the target of analysis. CORAS makes use of structured brainstorming where risks are identified by the identification and modeling of threats, vulnerabilities, threat scenarios and unwanted incidents, as well as the relations between these risk elements. The results are documented on-the-fly using CORAS threat diagrams.

Step 6: Risk estimation using threat diagrams. A risk is the likelihood of an unwanted incident and its consequence for an asset. The objective or the risk estimation is therefore to estimate the likelihoods and consequences of the identified unwanted incidents using the threat diagrams. However, the likelihood estimation also involves estimating the likelihoods for the identified threats to initiate threat scenarios, the likelihoods for the threat scenarios to occur, as well as the conditional likelihoods that scenarios can lead to unwanted incidents. By this additional information we get a stronger basis for estimating the likelihoods of the unwanted incidents (using the CORAS calculus), for identifying inconsistencies and possible mistakes or misunderstandings, and for identifying the most important sources of risk.

Step 7: Risk evaluation using risk diagrams. The risk evaluation involves the calculation of the risk levels resulting from the risk estimation and to determine which of the risks that should be evaluated further for possible treatment. The task is conducted using *CORAS risk diagrams*, and the risks are evaluated according to the risk evaluation criteria from the context establishment.

Step 8: Risk treatment using treatment diagrams. Risk treatment is the identification of means for cost-effective risk mitigation. For this task, the method makes use of *CORAS treatment diagrams* where options for risk treatment are annotated on the threat diagrams that depict the unacceptable risks. Risk treatment can be by means to reduce the likelihood and/or consequence of a risk, by avoiding the activities that lead to the risk, by transferring the risk to another party, or by retaining (accepting) the risk. A high level overview of the results of the risk treatment can be provided by using *CORAS treatment overview diagrams*.

6.3 ATM Security Risk Management Toolkit

The ATM Security Risk Management Toolkit [5] was developed by EUROCONTROL to support Air Navigation Service Providers (ANSPs) in identifying, assessing, documenting and managing security risks. The method is design to facilitate security risk management during the project development life cycle, in particular the initial phases of concept definition and feasibility studies.

The security risk management process involves conducting five subsequent activities, in addition to an initial optional step to decide whether a full security risk assessment is needed for the project in question. The method and its underlying terminology are based on ISO 31000 [9] and the ISO/PAS 22399 [8] standard on societal security. The method makes use of repositories, such as asset registers and attacker catalogues, and describes for each step the needed input and which output that shall be produced. More specifically, the method steps are as follows.

Step 0: Is a risk assessment required? The objective of this optional step is to identify projects that do not require a risk assessment, and to prioritize between projects that do.

Step 1: Define the scope of the system. The objective of this step is to define the system boundaries for the security risk assessment, develop the security goals, develop a system description, and identify the assets. This includes defining the areas which security should protect (such as safety, business or environment), the security goals of the ANSP, as well as other requirements such as legal and regulatory.

Step 2: Assess impact of a successful attack. The objective of this step is to identify which assets are relevant to the effective operation of the ANSP's ATM system, and the potential related incidents. The step uses the identified security goals and assets as input to assess the possible impact on security goals if the assets are attacked and harmed.

Step 3: Estimate likelihood of successful attack. The objective of this step is to estimate the likelihood of a successful attack on an asset. The attacks include those that originate from both outside and inside the system. In order to estimate the likelihood of successful attacks, the likelihood of attack attempts are estimated first. The estimation shall take into account any vulnerability that may be exploited, and the identified threat paths shall be documented as attack scenarios.

Step 4: Assess risks. The objective of this step is to identify the security risks for each attack. This includes specifying the risk appetite for the project (i.e. the risk evaluation criteria specified by a risk matrix), and to estimate risk levels by combining the likelihood and impact of each of the identified successful attacks.

Step 5: Define and agree management options. The objective of this step is to identify management options that reduce the risks to an acceptable level. The possible kinds of options are to terminate the activity that leads to unacceptable risk, to tolerate the risk, to transfer the risk, or to treat the risk by applying countermeasures or controls.

6.4 Comparison

A detailed comparison of the three selected methods is outside the scope of this deliverable, as our main objective here was the selection of these methods and the documentation of the criteria for the selection. Such a comparison is a main part of the forthcoming work of EMFASE that includes the development of the empirical evaluation framework and the concrete evaluation studies. The studies will target the criteria and parameters for method classification that we presented in Section 4. Using this classification as a basis, our aim is to develop a framework with techniques and means for evaluating and comparing risk assessment methods precisely with respect to such evaluation criteria.

There are, however, some obvious similarities and differences between the three risk assessment methods that alone make them interesting for comparison.

All methods are based on international standards. This is reflected by the processes they follow which, at a high level, are the same; after an initial description of the target and its scope, the risks are identified and evaluated, before options for risk mitigation are identified. They differ, however, regarding which standards that are the most important references. CORAS is based on ISO 31000, which does not target security in particular, although the method is compatible with more security oriented approaches like ISO 27005. The EUROCONTROL toolkit is also based on ISO 31000 standard, but has a focus on societal security and incident preparedness as specified by the ISO/PAS 22399 standard. SecRAM is the most information security oriented of the three as it is based on the ISO/IEC 27005 standard.

A difference between CORAS and the other two is that the former is model-driven and uses specific diagrams to support each task and the documentation of the results. All of the methods come with practical guidelines for how to conduct the risk assessments, including specifications of the required inputs and outputs at each step. However, where CORAS uses graphical models, the other two provides table templates to support the assessment and the documentation. This difference is interesting to investigate in the empirical studies to see how and to what extent it may affect the fulfillment of the criteria identified by the ATM stakeholders.

Another obvious difference between CORAS and the other two is that only the latter two targets the ATM domain in particular. There are therefore various kinds of support for ATM security risk assessment that only SecRAM and the EUROCONTROL toolkit provide. However, in the empirical studies all of the methods will be applied with the same additional support (such as repositories and descriptions of the analysis target), which allows us to study the differences between the methods in terms of the techniques, guidelines, documentation support, etc. alone.

For risk analysts, ATM professionals and other stakeholders, the time and resources available for conducting a risk assessment may impact the decision about which risk assessment method to use. As mentioned before, SecRAM is rather light weight and is designed to be applicable for personnel with little or no background in security and risk management. CORAS and the EUROCONTROL toolkit are for more thorough risk assessments, and may require more training. The balance between the required resources and expertise on the one hand and the desired results on the other hand is a timely topic of investigation during our empirical studies of the selected methods.

7 Risk Assessment Support

When conducting security risk assessments within the ATM domain – using SecRAM, CORAS or any other relevant method – there are various kinds of support that may or should be utilized. Some of these are provided by SESAR and provides specific support for the ATM domain, while others are of a more general kind. In the following we give a list of such relevant support.

ISO/IEC 27000 series on information security management. This ISO/IEC series of standards gives general guidelines for information security management, where the ISO/IEC 27005 standard concerns risk assessment in particular. In addition to describing the risk assessment process, the series provides the following relevant support.

- ISO/IEC 27001 list of control objectives and controls for information security management
- ISO/IEC 27005 list of assets
- ISO/IEC 27005 classification and list of threats
- ISO/IEC 27005 list of vulnerabilities

SESAR 16.02.0x and 16.06.02 projects. In addition to the SecRAM method itself, there is various supporting material from SESAR projects that are relevant.

- Project 16.02.03 SecRAM Implementation Guidance Material provides practical guidelines for how to conduct a security risk assessment using SecRAM
- Project 16.02.03 table templates to support the SecRAM assessment and documentation
- Project 16.02.05 Minimum Set of Security Controls (MSSC) that all operational areas shall adopt in order to reach a common minimum level of ATM security
- Project 16.06.02 develops a security register of assets, threats, vulnerabilities, threat scenarios and controls.

The CORAS approach. Some guidance material and supporting artifacts are freely available for users of the CORAS method.

- The CORAS tool can be downloaded from here: http://coras.sourceforge.net/downloads.html
- A video that gives a demo of how to get started using the CORAS tool is available here: http://coras.sourceforge.net/coras_tool.html
- A guided tour of the CORAS method can be downloaded from here: http://www.springer.com/cda/content/document/cda_downloaddocument/9783642123221-c3.pdf?SGWID=0-0-45-1010949-p173989983

8 Conclusion

In this deliverable we have presented our selected method objects of study for our development of the EMFASE framework for empirical evaluation of methods for security risk assessment for the ATM domain. The objective of EMFASE is to provide a framework that can be applied to any security risk assessment method that is adequate for this domain. However, as it in infeasible to conduct thorough studies of them all during the course of the EMFASE project, we need to select some representative methods.

Following the selection criteria presented in Section 5, we identified SecRAM, CORAS and the EUROCONTROL Security Risk Management Toolkit as good candidates for our objects of study; in addition to their relevance to the ATM domain, which is a crucial criterion, we have also within the consortium the required in-house expertise necessary for applying these methods and training any of the participants in the forthcoming empirical studies.

As a starting point for the selection we took into account the state of the art of security risk assessment methods (presented in Section 2), and we identified classification criteria based on data provided by relevant ATM professionals (presented in Section 3 and Section 4). Subsequently we identified the main selection criteria (presented in Section 5).

The selected methods will be applied in empirical studies where they are applied to ATM operational areas and use cases. The three methods in combination give a good coverage of the risk assessment features and techniques that we aim to study and evaluate. During the course of the project we will determine whether further methods, techniques or tools should be investigated as well, but this depends on our findings and research results, as well as any further research needs that we may identify.

The next step of the work of EMFASE WP1 is to develop the first version of the empirical evaluation framework. These initial results will be presented in deliverable D1.2, which is due at M12. The framework will elaborate and extend the initial criteria documented in this deliverable, based on existing practices, comparison of state of the art risk assessment methods, experimental studies, and further data gathered from ATM professionals.

9 References

[1] Agence Nationale de la Sécurité des Systèmes d'Information: EBIOS 2010 – Expression of Needs and Identification of Security Objectives (2010)

[2] Christpher J. Alberts and Audrey J. Dorofee: OCTAVE Criteria, Version 2.0. Tech. Rep. CMU/SEI-2001-TR-016, CERT (2001)

[3] Anselm L. Strauss and Juliet M. Corbin: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. SAGE Publications (1998)

[4] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2 – IT-Grundschutz Methodology, version 2.0 (2008)

[5] EUROCONTROL: ATM security risk management toolkit – Guidance material (2010)

[6] EUROCONTROL: ESSAR4 – Risk assessment and mitigation in ATM (2001)

[7] EUROCONTROL: Manual for national security oversight (2012)

[8] International Organization for Standardization: ISO/PAS 22399 – Societal security – Guideline for incident preparedness and operational continuity management (2007)

[9] International Organization for Standardization: ISO 31000 – Risk management – Principles and guidelines (2009)

[10] International Organization for Standardization / International Electrotechnical Commission: IEC 31010 – Risk management – Risk management techniques (2009)

[11] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 15408 – Common Criteria for Information Technology Security Evaluation (2009)

[12] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements (2005)

[13] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2008)

[14] Information Systems Audit and Control Association (ISACA): COBIT 5 - A business framework for the governance and management of enterprise IT. Rolling Meadows, ISACA (2012)

[15] Mass Soldal Lund, Bjørnar Solhaug and Ketil Stølen: Model-Driven Risk Analysis – The CORAS Approach. Springer (2011)

[16] Nancy R. Mead and Ted Stehney: Security Quality Requirements Engineering (SQUARE) Methodology. SIGSOFT Softw. Eng. Notes, 30(4)1-7 (2005)

[17] Daniel Mellado, Eduardo Fernández-Medina and Mario Piattini: Towards security requirements management for software product lines: A security domain requirements engineering process. Computer Standards & Interfaces, 30(6):361–371 (2008)

[18] Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence: The Security Risk Management Guide. Microsoft Corporation (2006)

[19] Ministerio de Administraciones Públicas: MAGERIT version 2 – Methodology for information systems risk analysis and management – Book I – The method (2006)

[20] National Institute of Standards and Technology: Guide for conducting risk assessments. NIST Special Publication 800-30, Revision 1 (2012)

[21] National Institute of Standards and Technology: Security and privacy controls for Federal information systems and organizations. NIST Special Publication 800-53, Revision 4 (2013)

[22] National Technical Authority for Information Assurance: HMG IA Standard No.1 – Technical risk assessment, Issue No: 3.51 (2009)

[23] Object Management Group: OMG Unified Modeling Language (OMG UML), Superstructure. Version 2.3. OMG Document: formal/2010-05-03 (2010)

[24] John Sherwood, Andrew Clark and David Lynas: Enterprise Security Architecture – A Business-Driven Approach. Tylor and Francis (2005)

[25] SESAR Joint Undertaking: SESAR ATM SecRAM implementation guidance material. Project deliverable 16.02.03-D03 (2013)

[26] SESAR Joint Undertaking: SESAR ATM security risk assessment method. Project deliverable 16.02.03-D02 (2013)

[27] SIEMENS Insight Consulting: CRAMM v5.1 – Information Security Toolkit. [ONLINE] Available at: http://www.ia.nato.int/niapc/DocumentGenerator/product/257/ManufacturersBrochure [Accessed 31 January 2014]

[28] Bruce Schneier. Attack trees. Dr. Dobbs Journal, 24(12):21–29 (1999)

[29] Guttorm Sindre and Andreas L. Opdahl: Eliciting security requirements with misuse cases. Requirements Engineering, 10(1):34-44 (2005)

[30] Frank Swiderski and Window Snyder: Threat Modeling. Microsoft Press (2004)

-END OF DOCUMENT-