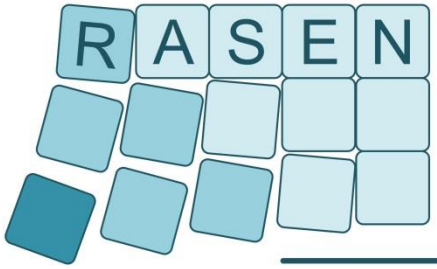

Compositional Risk Assessment and Security Testing of Networked Systems

Deliverable D5.3.3

Methodologies for Legal, Compositional, and Continuous Risk Assessment and Security Testing v.3

Project title:	RASEN
Project number:	316853
Call identifier:	FP7-ICT-2011-8
Objective:	ICT-8-1.4 Trustworthy ICT
Funding scheme:	STREP – Small or medium scale focused research project

Work package:	WP 5
Deliverable number:	D5.3.3
Nature of deliverable:	Report
Dissemination level:	PU
Internal version number:	1.0
Contractual delivery date:	2015-09-30
Actual delivery date:	2015-09-30
Responsible partner:	SINTEF

Contributors

Editors	Fredrik Seehusen (SINTEF), Bjørnar Solhaug (SINTEF)
Contributors	Jürgen Großmann (Fraunhofer), Tobias Mahler (UiO), Fredrik Seehusen (SINTEF), Bjørnar Solhaug (SINTEF), Ketil Stølen (SINTEF)
Quality assurors	Arthur Molnar (Info World), Fabien Peureux (UFC)

Version history

Version	Date	Description
0.1	15-02-10	Table of contents with partner roles
0.2	15-07-01	Input Fraunhofer
0.3	15-09-08	First full draft
0.4	15-09-17	Finalized for internal review
0.5	15-09-23	Updated after review
1.0	15-09-30	Final version

Abstract

This deliverable documents the application of the RASEN methodology within different processes and for different domains. The processes that are considered are established approaches to software development and security assessment so as to demonstrate the wider applicability and usefulness of the RASEN methodology. Two specific domains are moreover highlighted, namely cybersecurity and cloud sourcing. Both of these are highly relevant given the mainstream ICT infrastructures of today, and they both represent important current and emerging security challenges.
The deliverable presents WP5 results from the third and final year of the RASEN project regarding task T5.1 (Methodology for compositional and continuous risk assessment and security testing of large scale networked systems) and T5.2 (Methodology for legal risk assessment and security testing of large scale networked systems).

Keywords

Methodology; risk management; information security; cybersecurity; risk-based security testing; test-based risk assessment; compositional risk assessment; legal risk management; cloud sourcing

Executive Summary

This deliverable documents the main WP5 results from the third and final year of the RASEN project regarding task T5.1 (Methodology for compositional and continuous risk assessment and security testing of large scale networked systems) and T5.2 (Methodology for legal risk assessment and security testing of large scale networked systems).

The deliverable demonstrates the applicability of the RASEN methodology to established approaches to security assessment and system development. This shows the relevance of the RASEN technologies, and the benefit of complementing established approaches with the RASEN methodology. The deliverable moreover shows the applicability of RASEN to the highly relevant domains of cybersecurity and cloud sourcing. RASEN is a generic approach in the sense that it is developed for security risk assessment, security testing and compliance assessment in general. Whereas traditional ICT and information security is a core target domain of the RASEN methodology, RASEN is not limited to this domain alone. Finally, the deliverable presents a method for compliance risk assessment supported by natural language patterns and graphical modeling, as well as the evaluation of this method.

Table of contents

1 Introduction

This deliverable reports on the third and final year results of RASEN WP5 regarding task T5.1 (Methodology for compositional and continuous risk assessment and security testing of large scale networked systems) and T5.2 (Methodology for legal risk assessment and security testing of large scale networked systems). The deliverable first provides an overview of the RASEN methodology for combining security risk assessment, security testing and legal compliance assessment. This overall methodology is supported by the WP3 and WP4 techniques and tools for test-based security risk assessment and risk-based security testing.

A further purpose of this deliverable is to show the applicability of the RASEN methodology, techniques and tools to already established processes for system development and security assessment. In particular, we show how the RASEN methodology applies to and complements existing approaches, thereby demonstrating the viability of using RASEN both for secure system development and for security risk assessment of networked software systems.

In this deliverable we moreover explain the applicability of RASEN to the highly relevant domains of cybersecurity and cloud sourcing. The RASEN methodology is generic in the sense that it is applicable to security risk and compliance assessment in general. Although ICT and information security is often stressed, this does not mean that other domains are out of scope. Cybersecurity and security of cloud services is of particular relevance as their importance is constantly increasing in the information society of today. As substantiated in this deliverable, RASEN facilitates security testing, security risk assessment and compliance risk assessment also in these domains.

Finally, the deliverable presents the third year results regarding the development of the RASEN methods and techniques for the identification and assessment of compliance risk. The method is supported by natural language patterns, as well as a graphical modeling notation for deriving compliance risk models from the patterns. The application of the method to a cloud scenario is presented, along with an evaluation of the method in light of best practices.

The structure of the deliverable is as follows. In Section 2 we give an overview of the RASEN methodology and show three of its instantiations, namely risk-based compliance assessment, test-based security risk assessment and risk-based security testing. In Section 3 we show how the RASEN methodology relates to and complements existing approaches to security assessment and software system development. In Section 4 and Section 5 we explain the applicability of RASEN to the domains of cybersecurity and cloud services, respectively. Section 5 moreover presents the RASEN method for compliance risk assessment and its evaluation. Finally we summarize and conclude in Section 6.

2 Overview of the RASEN Methodology

Security risk assessment, security testing, and legal compliance assessment each contribute to an overall assessment of the security of a system. These activities are supported by existing standards such as ISO 31000[1], ISO 29119[2], and AS 3806-2006[3] but are normally treated as distinct areas that are isolated from one another. While the industry demands integrative approaches that cope with security as a whole, currently no standard exists that sufficiently emphasizes the systematic integration of security risk assessment security testing, and legal compliance.

The RASEN method addresses security risk assessments on different levels of abstraction and from different perspectives. Legal risk assessment especially addresses security threats in a legal context and under consideration of legal consequences. Security risk assessment specifically deals with the concise assessment of security threats, their estimated likelihoods and their estimated consequences for a set of technical or business related assets. Finally, security testing can be used to actually examine the target under assessment for vulnerabilities and its actual quality.

The RASEN method for risk-based security testing and legal compliance assessment is derived from ISO 31000 and slightly extended to highlight the identification and evaluation of compliance or security issues as one of the major tasks that need to be carefully aligned with typical risk assessment activities.

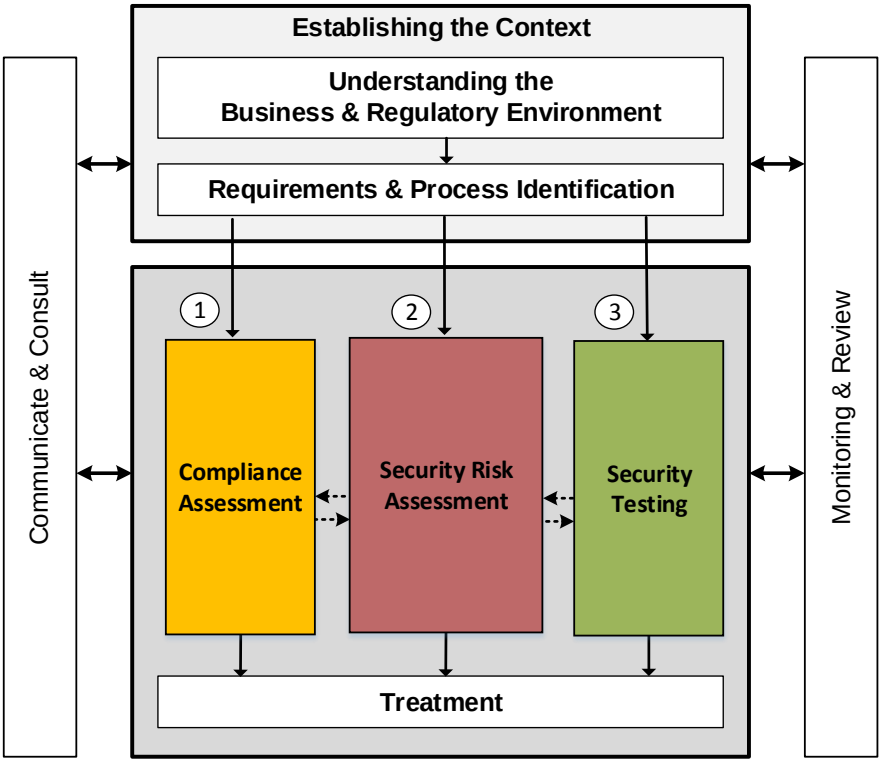

Figure 1 – Overall risk, compliance and security assessment process

Figure 1 shows the main activities of a combined risk assessment and security testing process. It starts with a preparatory phase called “Establishing the context“ and shows additional support activities like ”Communicate & consult” and “Monitoring and review” that are meant to set up the

[1] International Standards Organization. ISO 31000:2009(E), Risk management – Principles and guidelines, 2009
[2] International Standards Organization. ISO 29119 Software and system engineering - Software Testing-Part 1-4, 2012
[3] Australian Standard 3806-2006, Compliance programs (2006)

management perspective, thus to continuously control, react, and improve all relevant information and results of the process.

The process is generic and can be instantiated towards particular instances of integration. We consider three such integrations.

1. **A risk-based compliance assessment** process starts with the identification of compliance issues, and use risk assessment to identify, estimate, and evaluate compliance related risks.
2. **A test-based risk assessment** starts like a typical risk assessment process and uses test results to guide and improve the risk assessment. Security testing is used to provide feedback on actually existing vulnerabilities that have not been covered during risk assessment and allows risk values to be verified and adjusted based of tangible test result measurements.
3. **A risk-based testing** process starts like a typical testing process and uses risk assessment results to guide and focus the testing. Such a process involves identifying the areas of risk within the target's business processes and building and prioritizing the testing program around these risks. In this setting risks help focusing the testing resources on the areas that are most likely to cause concern or supporting the selection of test techniques dedicated to already identified threat scenarios.

In the following, we will describe these instances of integration in more detail.

2.1 Risk-based Compliance Assessment

The RASEN method is instantiated towards a systematic and risk-based approach to risk and compliance assessments. By systematic we mean that relevant risks and control measures are mapped, to the extent possible, to relevant compliance requirements. By risk-based we mean compliance requirements are prioritized based on their risk levels.

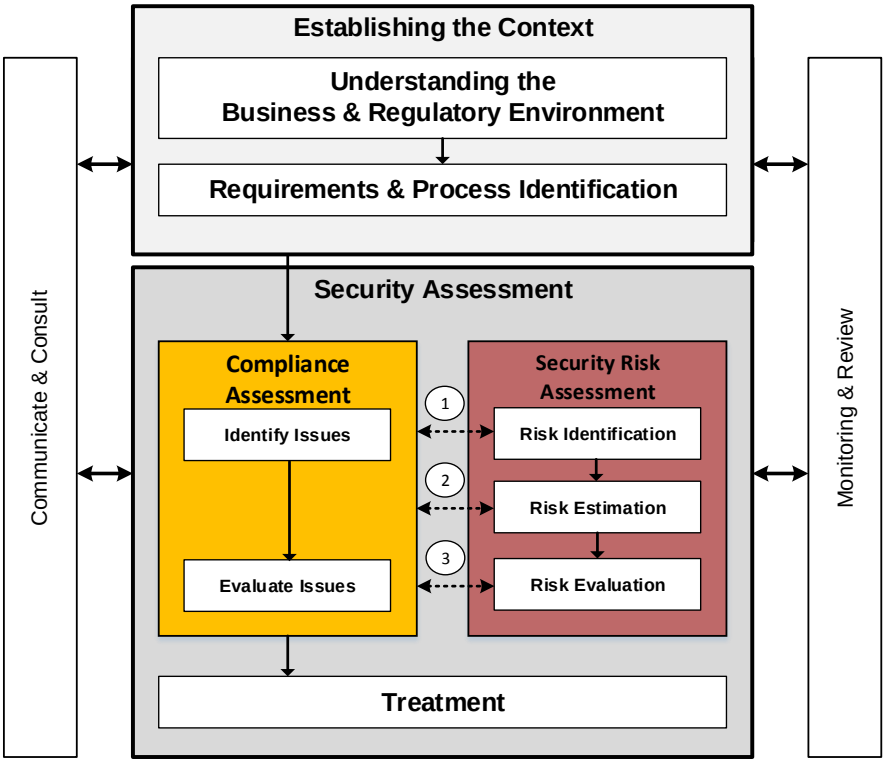

Figure 2 – Integrated risk and compliance assessment

Figure 2 shows the RASEN method instantiated towards risk and compliance assessment. In the following, we describe the main interactions between compliance and risk assessment.

1. **Compliance risk identification:** The main goal of the compliance risk identification is to deal with compliance requirements that imply risk. The RASEN approach provides a structured method for identifying risks from compliance requirements or from the business environment. This should also include identifying legal consequences of security risks.
2. **Compliance risk estimation:** A risk with a large potential loss and a low likelihood of occurrence is often treated differently from one with a low potential loss and a high likelihood of occurrence. However, in order to estimate the risk, one needs to understand the underlying uncertainty. That uncertainty can originate from a number of sources, including from the compliance requirements themselves. For example, compliance requirements may be unclear, or there may be uncertainty about the consequences of noncompliance.
3. **Compliance risk evaluation:** The risk evaluation step is used to prioritize compliance requirements based on their level of risk and to prioritize security risks based on their legal consequences. Prioritization may be relevant, for example, due to resource limitations.

2.2 Test-based Security Risk Assessment

The main purpose of integrating the testing process into the risk assessment process is to use testing to enhance some of the activities of the risk assessment process. This is achieved by ensuring that test results are used as explicit input to the risk assessment.

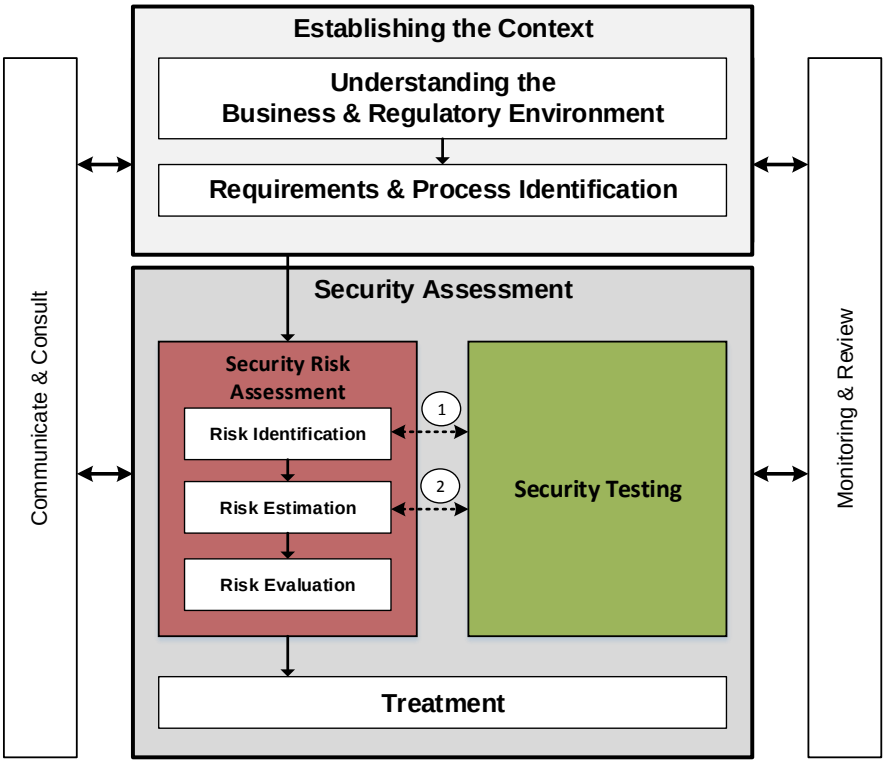

Figure 3 – Generic process for test-based risk assessment

Figure 3 shows how the unified RASEN process is refined into a process for test-based risk assessment. Here the risk assessment activity has been decomposed into the three activities of risk identification, risk estimation and risk evaluation. These three activities, together with the "establishing the context" and "treatment" activities form the core of the ISO 31000 risk management process. As indicated in Figure 3, there are in particular two places where testing can in principle enhance the risk assessment process.

1. **Test-based risk identification**: In a risk assessment process, the risk identification activity is performed with respect to a target of analysis, which is described and documented in the "establish context step". In a test-based risk assessment setting however, the risk

identification is not only based on the documentation of the target of analysis, but also on relevant test results of target of analysis. Particularly relevant in this setting is testing using automated testing tools such as vulnerability scanners or network discovery tools.

2. **Test-based risk estimation**: In a test-based risk assessment, the risk evaluation activity may be enhanced by test results (denoted (2) in Figure 3). At this point in the process, risks have already been identified and estimated, and the main reason for doing testing here is to gain increased confidence in the correctness of the risk model. In particular, the likelihood estimates of the risk model might have a low confidence if they e.g. depend on vulnerabilities whose presence in the target of analysis is unknown. By doing testing, we may investigate whether such vulnerabilities really are present in the target of analysis, and then use the test results to update the confidence level of the estimates of the risk model.

2.3 Risk-based Security Testing

Within the RASEN project, security testing is considered to be a systematic means to check the compliance of a system with its security specification. Risk-based security testing methods help to optimize the overall security testing process. The result of the risk assessment, i.e. the identified vulnerabilities, threat scenarios and unwanted incidents, are used to guide the test identification and may complement requirements engineering results with systematic information concerning the threats and vulnerabilities of a system. A comprehensive risk assessment additionally introduces the notion of likelihoods and consequences related to threat scenarios and unwanted incidents. These risk values can be used to identify which threat scenarios are more relevant for use as a starting point for testing.

The risk-based security testing process is structured like a typical security testing process. It starts with a planning phase, a test design & implementation phase and ends with test execution, analysis and summary. The result of the risk assessment, i.e. the identified vulnerabilities, threat scenarios and unwanted incidents, are used to guide the test planning, test identification and may complement requirements engineering results with systematic information concerning the threats and vulnerabilities of a system.

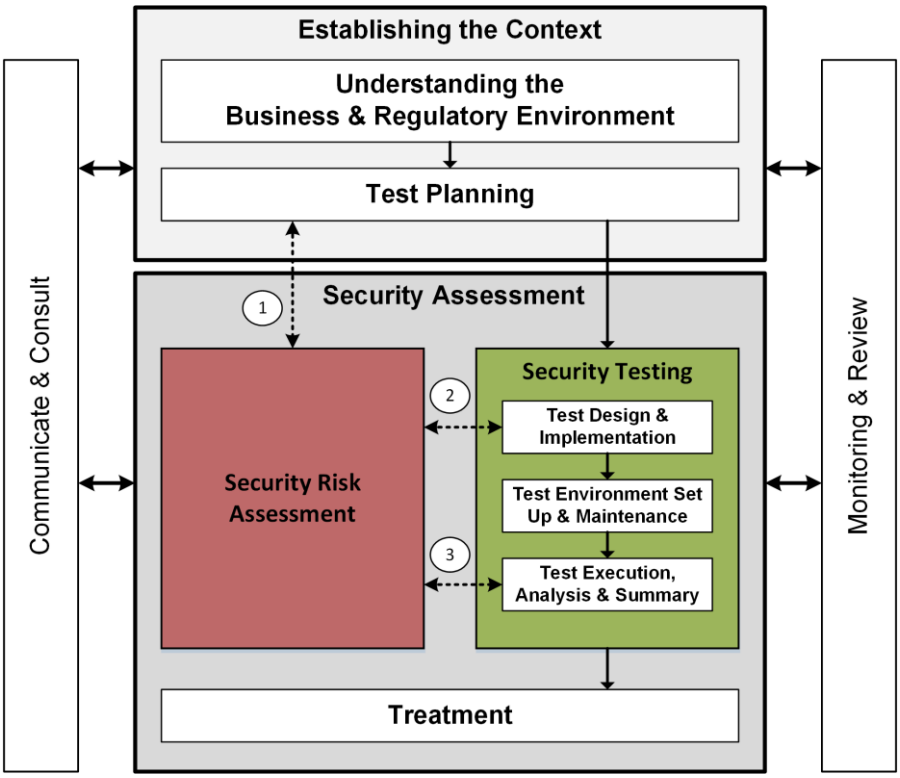

Figure 4 – Process model for risk-based security testing

Additional factors like probabilities and consequences can be additionally used to weight threat scenarios and thus help identify which threat scenarios are more relevant and thus identifying the ones that need to be treated and tested more carefully. From a process point of view, the interaction between risk assessment and testing could be best described following the phases of a typical testing process. Figure 4 illustrates the three phases of a testing process that are affected and supported by risk-based security testing.

1. Risk-based security test planning deals with the integration of security risk assessment in the test planning process.
2. Risk-based security test design, implementation deals with the integration of security risk assessment in the test design and implementation process.
3. Risk-based test execution, analysis and summary deals with a risk-based test execution as well as with the systematic analysis and summary of test results.

2.4 Conclusion

The RASEN method provides a comprehensive approach to cyber security management that takes into account technical as well as non-technical issues. The method integrates three areas that are traditionally addressed in isolation: security risk assessment, security testing, and legal compliance assessment. While the industry demands integrative approaches that cope with security as a whole, currently no other standard exists that sufficiently emphasizes the systematic integration of these three domains.

3 Applying the RASEN Methodology to Established Processes

The RASEN tool-supported methodology complements existing and established approaches to security assessment and secure software development. In particular, the RASEN methodology provides support that can be used to facilitate many of the tasks and steps of industry best practices.

One of the well-known principles in system development is the principle of composition and decomposition [46]. Decomposition is the process of partitioning a system specification into separate modules that can be developed, analyzed and validated independently, thus breaking the development problem into more manageable pieces. Moreover, each module may be developed at different sites, by independent teams, or within different companies [45]. Composition is the opposite process. The term refers to the systematic integration of parts to realize the overall system or a system of systems. This section provides guidance in applying the security assessment principles defined by the RASEN Method (see Deliverable D5.3.2 [42]) to a typical system life cycle where decomposition and composition principles play a major role. In such a setting, the security assessment process itself must be compositional.

A compositional process to security assessment should initially follow the same procedure for individual parts as the (non-compositional) security assessment process for the whole system. The main difference is that the system is decomposed into components or parts and that these components are assessed individually. This has several advantages. It allows considering specific contextual and technical details that become only visible when a system is broken down into several functional parts. Moreover, it supports processes with large integration efforts where multiple software or component suppliers deliver individual parts of a system. For each of these components there can be a separate risk assessment that will be integrated to form the overall system's view.

In the following subsections this is substantiated by showing how the RASEN method applies to established processes and risk assessment approaches.

3.1 Integration within the Software Development Lifecycle

Integrating and interweaving security risk assessment and security testing allow for a more precise, focused and dynamic security assessment of systems. Generally there are two ways to combine security testing and security risk assessment.

- A process for risk-based security testing in which risk assessment results are used to guide and focus the testing activities. The identified risks help focusing the testing resources on the areas that are most likely to cause concern. Results from threat and vulnerability analysis can be used to ease the selection of dedicated test techniques and test cases that precisely address already identified risks.
- A process for test-based risk assessment where systematic security testing and the respective test results are used to improve the risk assessment results. Security testing may provide feedback on actually existing vulnerabilities that have not been covered during risk assessment. Moreover it allows to adjust risk values on basis of tangible measurements like test results. Security testing could provide a concise feedback whether the properties of the target under assessment have been really met by the risk assessment.

As depicted in Figure 5, risk-based security testing and test-based risk assessment can be applied in different phases and to different testing activities in the system life cycle.

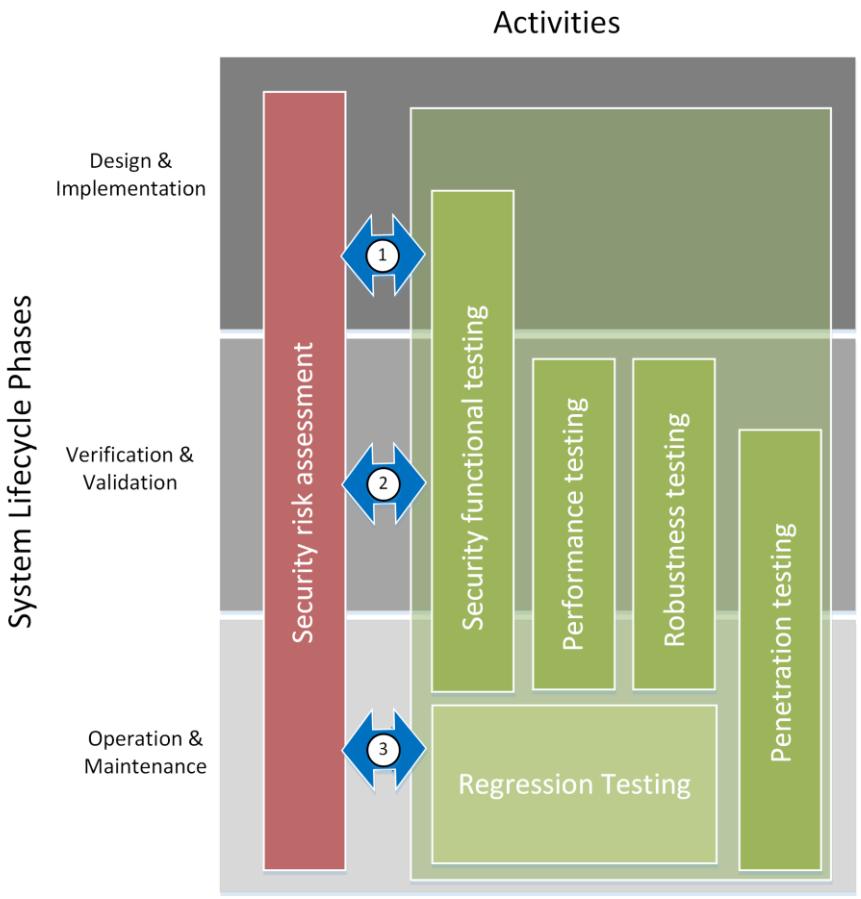

Figure 5 – Risk-based security testing as systematic combination between security risk assessment and security testing.

1. During design and implementation risk-based security testing and test-based risk assessment should focus the integration between security risk-assessment and security functional testing. The main points of reference are security functional requirements and the verification of their implementation by testing. The notion of risk might help focus the implementation and testing efforts for all development driven testing activities (e.g. module and unit testing).
2. During the verification and validation phase it can (but not necessarily will) be extended to also cover other security testing activities like performance testing, robustness testing and penetration testing. Risk-based security testing should be used to focus the test design and test implementation efforts, to choose the appropriate testing techniques and to communicate test results in the context of the product's security risks.
3. During the operation and maintenance phase the focus slightly changes. Penetration testing is used to discover new and unknown vulnerabilities. This activity can especially help identify new risks and thus improve the risk assessment as described in test-based risk assessment approaches. Regression testing is usually used to verify whether a changed system still meets the original security requirements with respect to functionality, performance and robustness. These activities can most probably be optimized by means of risk-based security testing.

Figure 6 illustrates the application of decomposition and composition in a typical software development life cycle. The target of analysis is assessed as a whole at the beginning, and is assessed in parts or components when the target is decomposed into several parts or components. Risk assessment, security testing and the integration thereof follow in principal the same decomposition/composition strategy as the target of assessment itself.

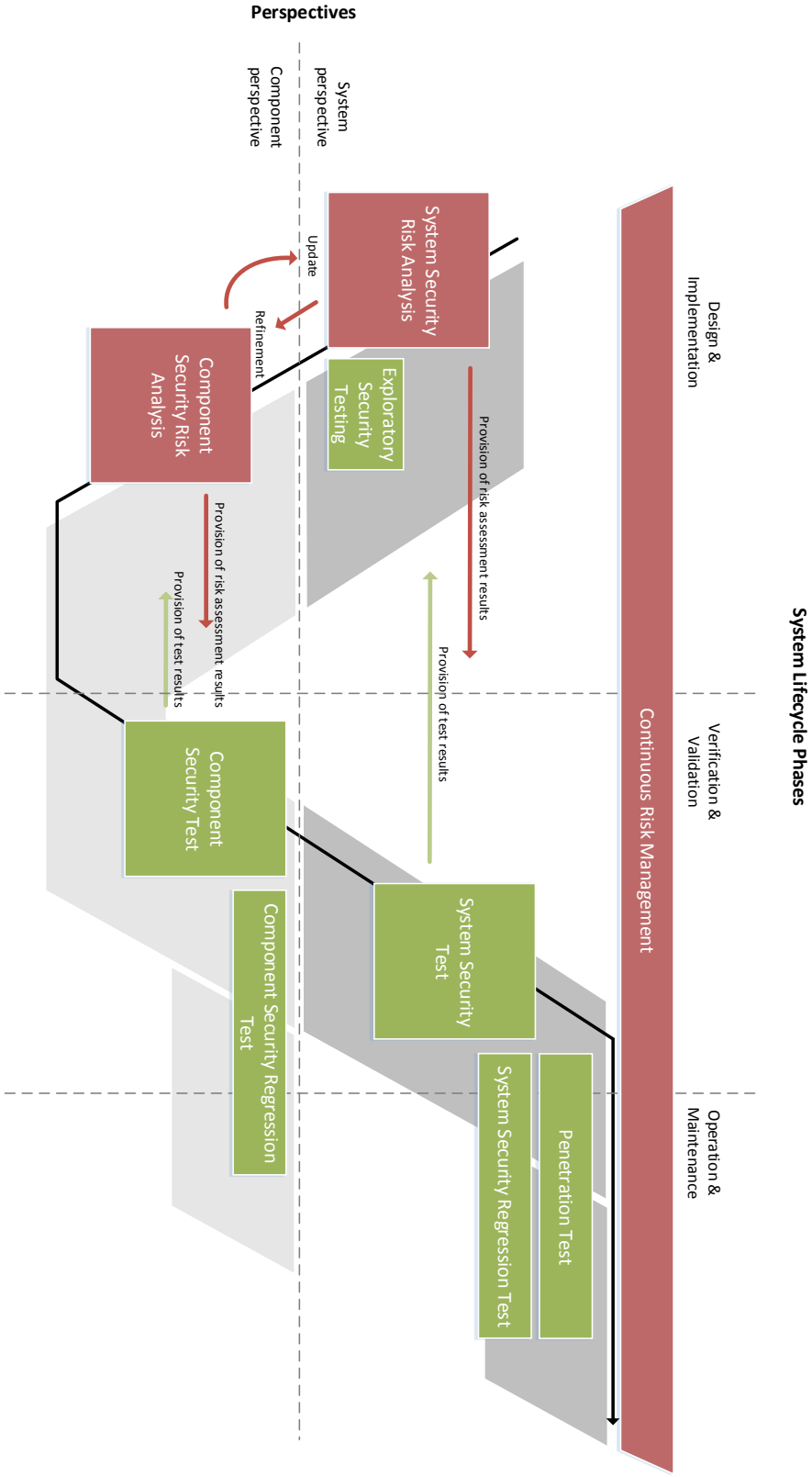

Figure 6 – Overview of a risk assessment process with composition/decomposition

3.1.1 System Security Risk Assessment

The overall process should start by taking the system's perspective. The security risk assessment (SRA) follows the risk assessment process that is described in RASEN deliverable D5.3.2 [42] by going through the risk identification, risk estimation and risk evaluation phases. The system security risk assessment targets risks for the whole system, thus system wide assets and incidents are considered. The interaction with security testing should in general follow the rules defined for test-based risk identification and test-based risk estimation (see D5.3.2). If there is no established security testing process at that time, there might be a dedicated exploratory testing phase, which is driven by the risk assessment and only meant to provide dedicated testing feedback to the risk assessment. However, at an early time in a system development process, there might often neither exist an established security testing process nor an executable system. In this case, the feedback from the security testing should be postponed until a functional system is available.

3.1.2 Component Security Risk Assessment

After having completed the risk assessment for the overall system, the system is typically decomposed into parts. In principle, the decomposition is driven by the development process and respects modularization requirements that come from the system's architecture or that are determined by integrator/supplier relationships. In other words, component security risk assessment should follow the same decomposition approach as the system development process. In fact, each of the major components that have been defined during system development should be assessed on their own. However, clustering of components is allowed and might help to focus efforts on the major architectural items. In contrast to system risk assessment, the focus of the assessment should move towards an assessment of the technical properties for each of the components. Thus, vulnerability assessment and the assessment of the technical impacts should get much more attention than threat and asset identification. Threat and asset identification is usually done on system level and should be deliberately reused when the component perspective is taken.

3.1.3 Refinement and Update Process

The two processes of the system security risk assessment and the component security risk assessment belong together. The relation between them should be seen as an iterative refinement and update process. Security risk assessment provides the overall context. It identifies the high level assets (e.g. often determined by the business context of the system) and defines the overall threats, threat scenarios, vulnerabilities and unwanted incidents. The component security risk analysis allows for a deeper understanding of the technical causes and impacts focusing on vulnerabilities and unwanted incidents. Since component risk analysis is carried out at a later point in time, there is much more system related information available (e.g. interface definitions, details of realization). This information can be used to allow for a better localization and specification of vulnerabilities, unwanted incident and their impact on and propagation to other parts and components of the system.

Similar to system security risk assessment, the interaction between component security risk assessment and security testing should in general follow the rules defined for test-based risk identification and test-based risk estimation. In contrast to security risk assessment it can be considered that there is already an established security testing process at that time of the process, so that a dedicated exploratory testing phase, with the only purpose to provide dedicated testing feedback to the risk assessment, should not be carried out. Instead, the component security risk assessment should be carried out, having already the component security testing phase in mind. Thus, assessment results and reports should be structured in such a way that they serve as input for the security testing process according to the risk-based security testing section in deliverable D5.3.2. Finally, component security risk assessment results should be used to update the system security risk assessment with respect to estimates on probabilities, identified vulnerabilities and technical impact.

3.1.4 Security Testing

Security testing should start when the security risk assessment already has gone through its first iteration. Thus, first risk assessment results are available for the system's perspective as well as for the component's perspective. Security test planning should be done according to our proposal for risk-

based security test planning and cover both perspectives, i.e. the security system testing as well as security component testing phase. Security component testing should be used to test for vulnerabilities and the correctness of security features on component level. System security testing should be used to test the integrated system, cover integration & configuration related vulnerabilities and ensure (as far as testing alone can ensure) the functional correctness of the high level security features. The interaction with security risk assessment should in general follow the rules defined for risk-based security testing. While system security testing should especially interact with system security risk assessment, security component testing should interact with component security risk assessment[4].

The overall process that is described above should be considered as a highly iterative process. System security risk assessment should be used to focus the component security risk assessment activities as well as the system security testing activities. In return both process, the component security risk assessment process as well as the system security testing process, provide updates for the system security risk assessment. Similar, component security risk assessment should be used to directly improve the component security testing activities. In return, the results from component security testing should be used to update the component security risk assessment and thus, transitively, the system security risk assessment.

Independent of the system life cycle phase the testing is carried out (i.e. the verification & validation phase or in the operation & maintenance phase). Test planning, test design and test summary and execution should keep their relation to security risk assessment as described for the risk-based security testing process in deliverable D5.3.2. An overall risk management process should ensure that the risk assessment on the different levels, as well as the integration of the testing activities, are kept up to date and are coordinated.

3.2 Mapping Between ETSI eTVRA and the RASEN Method

The ETSI Threat Vulnerability and Risk Analysis (eTVRA) [54] method is used as a tool to identify potential risks to a system based upon the likelihood of an attack and the impact that such an attack would have on the system. ETSI eTVRA is carefully aligned with ISO 31000 and ISO 27000 and thus provides the fundamental justifications for the development of standards based security solutions. An overview of the eTVRA steps is shown in Figure 7.

[4] Please note, especially when it comes to component level testing, static testing activities like source code, analysis should be used in addition to dynamic testing. Static testing activities have a quite good discovery rate for a larger number of known vulnerabilities

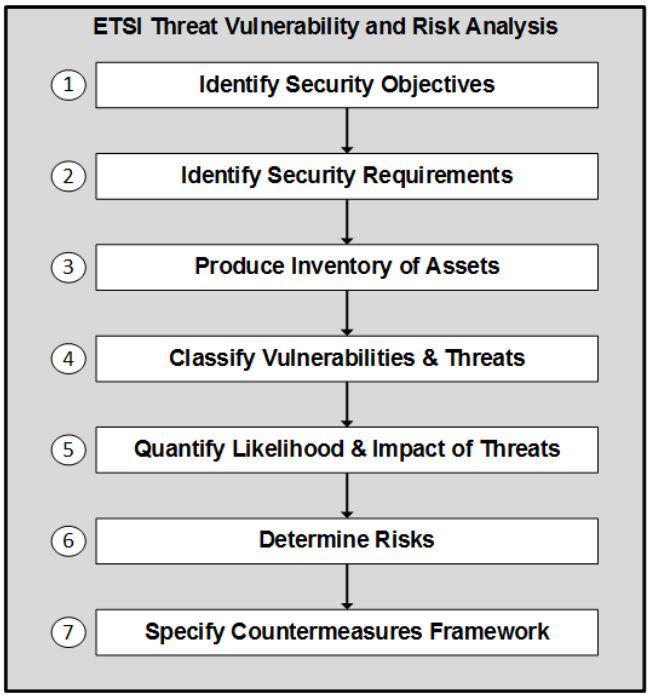

Figure 7 – The eTVRA Method

The eTVRA method involves a systematic 7-step process for identifying potentially damaging incidents within a system and specifying countermeasures to prevent such incidents from occurring. Within this section we show how the principles developed for the RASEN method could be directly integrated and mapped with ETSI eTVRA. Table 1 shows the mapping between the ETSI eTVRA activities and its equivalent in the RASEN method. If we see certain benefits, when specific RASEN techniques are applied, we have described the benefit in the third column.

ETSI eTVRA activity	RASEN method activity	RASEN method benefit
Identify Security Objectives	**Establishing the Context:** Understanding the business & regulatory environment**.**	
Identify Security Requirements	**Establishing the Context:** Requirements & Process Identification.	
Produce Inventory of Assets	**Test-based security risk assessment:** Risk Identification	
Classify Vulnerabilities & Threats	**Test-based security risk assessment:** Risk Identification	The RASEN activities *test-based attack surface analysis* and *test-based vulnerability identification* use security testing to obtain information about the attack surface and the presence of actual vulnerabilities in the target of evaluation.
Quantify Likelihood & Impact of Threats	**Test-based security risk assessment:** Risk Estimation	The RASEN activities *test-based likelihood estimation and Test-based estimate validation* use security testing to obtain information which can support the estimation of the likelihood that an attack will be successful if initiated.

		Security testing is most often used for identifying vulnerabilities, and the presence of these has a direct impact on this likelihood.
Determine Risks	**Test-based security risk assessment:** Risk Evaluation	
Specify Countermeasure Frameworks	**Treatment**	

Table 1 – Mapping of activities from ETSI eTVRA and activities of the RASEN method

3.3 Mapping Between Microsoft SDL and the RASEN Method

The Microsoft Trustworthy Computing Security Development Lifecycle (Microsoft SDL) [48] is an approach to develop secure software. It has been released by Microsoft in 2004 and is aimed at software developers who develop software that must withstand malicious attacks.

Microsoft's principle is "security by design". It aims for integrating software security as an explicit requirement in the development process. Generally, SDL includes security measures and best practices that complement the traditional software development process that ensures to consider and integrate security to the extent it is necessary. The security measures are aligned with classical the development steps as depicted in Figure 8.

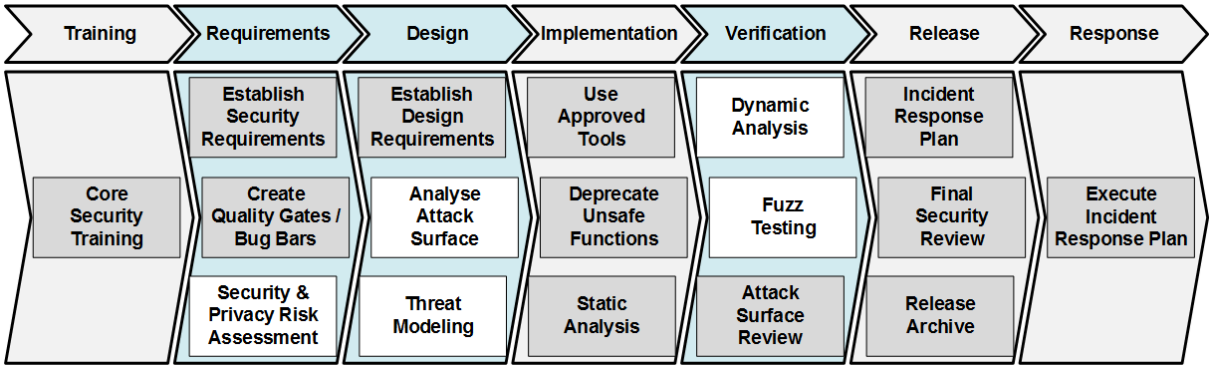

Figure 8 – The Microsoft Security Development Lifecycle

Since the RASEN method aims for improvements in security risk assessment and security testing, it only affects activities in the Requirements, Design and Verification phases of a classical software development process and thus also in Microsoft SDL. Figure 8 highlights the activities in Microsoft SDL that are covered by the RASEN method and are directly affected and improved by applying the RASEN techniques. Table 2 shows the integration of RASEN method processes in Microsoft SDL.

RASEN method	SDL Phase & Activity	RASEN method benefit
RASEN test-based risk assessment: the RASEN process for test-based risk assessment aims for an assessment of security & privacy risk in an iterative process that combine risk assessment with testing. The overall process	**Requirements:** *Security & Privacy Risk Assessment*	The RASEN process for test-based risk assessment comprises all activities required for risk assessment.
	Design: Analyze Attack Surface	The RASEN activity *test-based attack surface analysis* use security testing to obtain more precise information about the attack in the target of evaluation.
	Design: Threat	The RASEN activity *test-based vulnerability*

contains activities like attack surface analysis and threat modeling that are also referred in Microsoft SDL.	Modelling	*identification* use security testing to obtain more precise information on the presence of actual vulnerabilities in the target of evaluation and thus allows for a more precise threat analysis.
RASEN risk-based security: the RASEN process for risk-based security testing aims for organizing all relevant security testing activities during the validation phase of a SDL.	**Verification:** *Dynamic Analysis*	The RASEN process for risk-based security comprises all activities required for the dynamic validation of a software system. Additionally, risk assessment results are used to guide and focus testing activities on those areas that are most likely to cause concern. Results from threat and vulnerability analysis are used for the selection of dedicated test techniques that precisely address already identified risks.
	Verification: *Fuzz Testing*	See above (Fuzz Testing is a dedicated testing techniques and thus below the level of specification of the RASEN method. However, Fuzz testing can be improved when combined with risk assessment as proposed by the RASEN process for risk-based security testing.

Table 2 – Mapping of activities from Microsoft SDL and activities of the RASEN method

4 Applying the RASEN Methodology to the Cybersecurity Domain

As depicted in Figure 1, security risk assessment is a core element of the overall process of the RASEN methodology. Although the RASEN methodology and supporting tools and techniques have not been developed for coping with cybersecurity in particular, the method is very well positioned and suitable for cyber-risk assessment. Whereas RASEN focuses on the security of networked software systems, which is not exactly the same as cybersecurity, the processes and techniques are applicable also to the latter. The purpose of this section is to position the RASEN methodology with respect to cybersecurity, and to explain how RASEN facilitates cyber-risk assessment.

We start by giving a brief introduction to cybersecurity and explaining how cybersecurity relates to information security and critical infrastructure protection. Next we introduce the process for cyber-risk assessment, and we explain how RASEN supports each of the steps of this process. For a more detailed introduction to cybersecurity and cyber-risk assessment in particular, we refer to our publication on this topic [50].

4.1 Cybersecurity

Cybersecurity should not be confused with information security, ICT security or Internet security, although there often is considerable overlap. In order to precisely understand what cybersecurity is, we need to understand what we seek to protect and what we seek to protect from.

We refer to the systems of concern as ***cyber-systems***, which are systems that make use of a cyberspace. A ***cyberspace*** is a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as all information in storage or transit. For most organizations and other stakeholders, cyberspace is for all practical purposes synonymous with the Internet, which is a global cyberspace in the public domain [48][51]. Our definition of cyberspace is more general to allow for other collections of interconnected networks, such as military networks, emergency communication networks and other kinds wide area networks (WAN).

Note that risks that stem from or are due to a cyberspace, such as the Internet, may have implications beyond the cyberspace alone; a cyber-system may include information infrastructures, as well as people and other entities that are involved in the business processes and other behavior of the systems. This means that cyber-systems are part of the organizational structure of most organizations. Cyber-systems have moreover become more and more ubiquitous in society at large, and many critical infrastructures are cyber-systems.

Hence, while cybersecurity may involve the security of a cyberspace itself, most organizations are concerned with the protection of their own cyber-systems from cyber-threats. Both of these concerns are nevertheless within the scope of our definition, namely that ***cybersecurity*** is the protection of cyber-systems against cyber-threats. A cyber-threat arises via cyberspace, and is therefore a threat that any cyber-system is exposed to. We define a ***cyber-threat*** as a threat that exploits a cyberspace. Examples of malicious cyber-threats are DoS attacks and injection attacks that are caused by intention, whereas system crash due to programming error is an example of a non-malicious threat.

Notice, importantly, that what defines cybersecurity is not what we seek to protect, but rather what we seek to protect from; in other words, our concern is not the kinds of assets that are to be protected, but rather the kinds of threats to assets. In order to further clarify the notion of cybersecurity, we relate it in the following to the notions of information security and critical infrastructure protection.

4.2 Cybersecurity, Information Security and Critical Infrastructure Protection

The RASEN methodology applies to multiple domains, including cybersecurity, information security and critical (information) infrastructure protection. Within the RASEN project, this is concretely demonstrated via the use cases of WP2. Although there is considerable overlap between these domains of security, they are not identical.

Information security is the preservation of confidentiality, integrity and availability of information [22]. Information can come in any form, be it electronic or material, or even as the knowledge of personnel. In order to ensure information security, information in all formats must be protected from threats of any kind, be it physical, human or technology-related threats. Cybersecurity, on the other hand, concerns the protection from threats that exploit cyberspace. Such threats may target information assets, which is why information security is an important part of cybersecurity. However, cybersecurity concerns only those information assets that can be targeted via cyberspace. Cybersecurity is moreover not limited to the protection of information assets alone; it often involves infrastructure protection, and may also include the protection of assets such as life, health, reputation and revenue. Hence, while there is considerable overlap, these two domains of security go beyond each other.

Infrastructure security, or critical infrastructure protection (CIP), is concerned with the prevention of disruption, disabling, destruction or malicious control of infrastructure [48]. Examples of such infrastructures are telecommunication, power supply, banking and finance, and emergency services. Many critical infrastructures make use of a cyberspace and are therefore cyber-systems. Hence, the security of such systems often involves protection from cyber-threats. CIP in general, however, goes beyond cybersecurity since CIP involves the protection of any critical infrastructures, whether or not it makes use of a cyberspace. Cybersecurity, on the other hand, concerns the protection of infrastructures that can be targeted via a cyberspace, such as telecommunication systems or a smart grid.

How cybersecurity relates to information security and CIP is illustrated by the Venn diagram in Figure 9. The figure shows that while cybersecurity may involve both information security and CIP, the former is not simply a combination of the latter two.

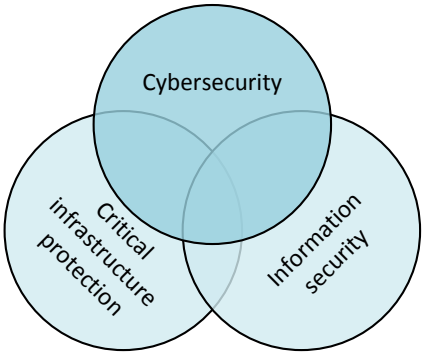

Figure 9 – Cybersecurity vs. information security and CIP

4.3 Cyber-Risk Assessment Using the RASEN Method

For a detailed introduction to cyber-risk management and cyber-risk assessment, we refer to our publication on this particular topic [50]. The purpose of this section is to give a brief account of how the RASEN methodology can be instantiated in the cybersecurity domain, and how the RASEN techniques facilitate cyber-risk assessment.

The cyber-risk assessment process is a specialization of the standard risk assessment process as defined in the ISO 31000 risk management standard. Following the risk assessment terminology of Section 2, cyber-risk assessment includes the steps as shown in Figure 10.

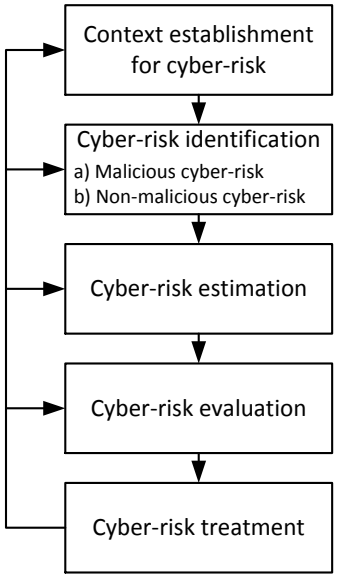

Figure 10 – Process for cyber-risk assessment

The most obvious difference from the general case is the separation of the risk identification step into two, namely identification of malicious cyber-risk and identification of non-malicious cyber-risk. We say that a cyber-risk is malicious if it is caused by a malicious threat, such as a DoS-attack of a malware injection, and that it is non-malicious otherwise. The reason for dealing with them separately is that they are very different in nature. In order to understand malicious threats, we need to consider things like motive, skills, resources, intentions, and so forth. Non-malicious cyber-risks, on the other hand, are usually not intended and rather happen due to errors, insufficient awareness, weak routines, and the like. In the following we go through each step in turn.

4.3.1 Step 1: Context Establishment for Cyber-Risk

The context establishment of the RASEN process is already well adapted to the setting of cyber-risk assessment. A particular concern is that we need to understand how the cyber-system in question makes use of and interacts with cyberspace. For an online eHealth or banking service, for example, how can the system be accessed over the Internet, which services and what information are transmitted, who are the remote users and roles? This gives a basis for understanding how and where cyber-threats arise, and which assets are relevant. As part of the description of the target of assessment, we therefore include the interface to and interaction with cyberspace and other relevant parts of the environment. This interface overlaps with the attack surface, which is the attack entry points and also where information and data can get out.

Typical assets of concern in the setting of cyber-risk assessment are information and information infrastructures. But we also need to take into account assets that can be harmed as a further consequence, such as reputation, market share, revenue, privacy and legal compliance. All these particular aspects are clearly seen to using the RASEN tool-supported methodology.

4.3.2 Step 2: Cyber-Risk Identification

For the identification of malicious cyber-risks, we need to identify the possible malicious cyber-threats, the vulnerabilities they may exploit, as well as the incidents they cause. The RASEN methodology is well suited for this task by the systematic use of cyber-threat and vulnerability repositories (like CAPEC and CWE), the specification and use of security test patterns, the active use of security and vulnerability testing, as well as the generation of risk models based on available attack patterns.

For the identification of non-malicious cyber-risks, RASEN makes use of established techniques such as brainstorming and interviews, as well as any available data such as logs, monitored data, statistics, and system specifications. Additional useful resources with lists of threats and vulnerabilities are, for example, ISO 27005 [47] and the NIST risk assessment guide [49].

4.3.3 Step 3: Cyber-Risk Estimation

There are two aspects that in particular distinguish the estimation of cyber-risk from risk estimation in general. First, for malicious threats where there is motive and intent behind, it can be hard to estimate the likelihood of occurrence and the consequences of incidents. Second, due to the nature of cyber-systems we have several options for logging, monitoring and testing that we can benefit from. There are moreover various open repositories that we can make use of. These aspects are very well addressed by the RASEN methodology.

For example, RASEN makes use of the MITRE repositories of attacks (CAPEC) and vulnerabilities (CWE) to gather estimates of typical likelihoods and consequences, as well as lists of typical kinds of consequences such as loss of integrity or consequences. While such estimates are used as initial values by the RASEN methodology, they are always adjusted to take into account the target system, the assets and the stakeholder in question. Moreover, supported by security testing patterns and attack patterns, RASEN makes systematic use of testing to facilitate the risk estimation. The RASEN methodology also uses the results to further guide the testing process and select the test cases that are likely to provide the most valuable information to the risk assessors.

4.3.4 Step 4: Cyber-Risk Evaluation

Risk evaluation involves determining which risks need to be considered for treatment by comparing the risk estimates with the risk evaluation criteria. This is conducted the standard way also for cyber-risk assessment, and when following the RASEN methodology. One issue, however, that is very relevant in the domain of cybersecurity is that of uncertainty. If the basis for estimating risks is insufficient or imprecise, we may not be able to decide whether or not identified risks are acceptable.

RASEN is well suited for tackling this issue as uncertainty is explicitly documented in the risk models and taken into account in the security risk assessment process. If the risk levels and their associated uncertainty estimates are such that decisions regarding security and risk treatment cannot be made, the risks in question need to undergo further assessment following the RASEN methodology. The additional assessment can be conducted by a new iteration of the cyber-risk assessment steps so as to gather more information. To this end, RASEN has the advantage that the explicit uncertainty estimates, together with the initial risk estimates, are used to guide the process and identify areas to be investigated further. In particular, the RASEN methodology facilitates the identification of security test cases that are most likely to provide the needed additional information.

4.3.5 Step 5: Cyber-Risk Treatment

Risk treatment is to identify and implement cost-efficient means for mitigating risks and keeping the residual risks at an acceptable level. There are two aspects that are particularly specific to the domain of cybersecurity. First, due to the highly technical nature of cyber-systems, the means for risk treatment are also largely technical. We moreover need to take into account the human involvement and the sociotechnical aspects of the systems. Second, we need to take into account that malicious threats may be hard to eliminate due to their nature, and that a great many threat sources are outside the system and can reside almost anywhere.

The RASEN techniques for risk assessment facilitate the treatment identification in both these respects. The systematic use of security test patterns and attack patterns that are instantiated for the target of assessment in question generates extensive and concrete information about the kinds of threats and vulnerabilities that are most relevant. Moreover, the test results and the risk models detail the picture further with information such as the likelihood of an attack to be successful and the degree to which a vulnerability can be exploited.

A further advantage of the RASEN methodology regarding cyber-risk assessment is that the process yields a good understanding and documentation of the cyber-system at hand, including the parts and aspects that are critical for its security. This understanding and documentation is valuable not only for the treatment of cyber-risk, but also for the ongoing and more general management of cyber-risk and cybersecurity. In particular, the RASEN tool-supported methodology provides stakeholders with better insight into cyber-security issues regarding applications, servers, clients, networks, and so forth. The documentation of the interface to cyberspace and the attack surface of the system in question is also valuable information in this respect.

4.4 Conclusion

The RASEN methodology (see Section 2 for an overview) has been developed to enable a systematic integration of security risk assessment, security testing and legal compliance of networked software systems. Although the RASEN methodology, including techniques and tools, has not been developed for cybersecurity in particular, the methodology is still well suited and highly applicable for the purpose of cyber-risk assessment. This is obviously witnessed by all of the RASEN case studies that are from industrial application domains of critical infrastructures that are exposed to cyber-threats.

In this section we have given a brief introduction to cyber-risk assessment for the purpose of positioning RASEN in the context of cybersecurity. We have focused on some of the core issues of cyber-risk assessment as compared to risk assessment in general. We have explained how the RASEN methodology and techniques are well aligned with these issues, and how they provide risk assessors and stakeholder organizations with the necessary means for assessing, understanding and documenting cybersecurity risks.

5 Applying the RASEN Methodology to Support Compliance Assessments in Cloud Sourcing

In this section we document the third year results regarding the development of the RASEN method for compliance risk assessment. We present the application of the method and techniques to a cloud sourcing scenario, as well as the evaluation of the method in light of best practices.

5.1 RASEN in Light of Best Practices on Compliance and Risk Assessment

Current best practices in compliance and risk assessment involve two separate processes. Generally, the compliance assessment process involves the identification of relevant requirements, their evaluation and taking measures for their implementation in the form of policies and procedures. This is often followed by regular checks on whether these measures are adequate. On the other hand, the risk assessment focuses predominantly on business level risks, i.e. operational, technical. This represents two separate approaches working independently as depicted in Figure 11. These approaches work well in many contexts and our approach does not aim to replace these. The aim of RASEN is to explore and evaluate an alternative to the current practices.

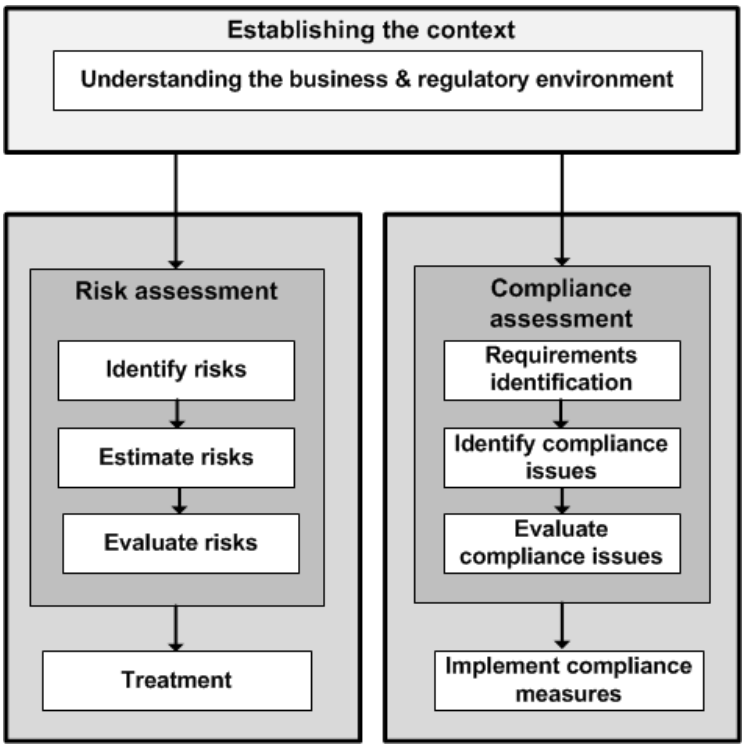

Figure 11 – Best practices of risk assessment and compliance assessment

One of the objectives behind the RASEN method is to integrate the compliance assessment and risk assessment so that the risk assessment is used to make decisions regarding compliance in a risk perspective. From a compliance point of view, conducting a risk assessment could serve two major objectives. First, the risk assessment might help to deal with compliance requirements that imply risk. Compliance requirements may be unclear, or there may be uncertainty about the consequences of noncompliance. Thus, the risk assessment can help to deal with uncertainty resulting from legal or other requirements. Second, the risk assessment can be used in order to prioritize compliance measures based on risks. Prioritization may be relevant due to resource limitations. Thus, the risk

assessment enables to focus the compliance resources on the areas that are most likely to cause concern. However, risk management is a challenging cognitive exercise because it involves the identification and assessment of “complex set of statements about” future events together with their likelihood and consequence estimation [28]. Such an exercise is even more challenging when it involves identifying and assessing the likelihood of “legal outcomes” [28].

In other fields, the solution to such challenges partly lies in using software tools, which aim at simplifying the assessment and communication of risks [28]. For example, an eHealth service provider might wish to assess the risk of a particular technical failure leading to liability according to a specific law or contract. In this context, conducting compliance risk analysis would benefit from the joint participation of experts from different disciplines, including legal experts, security experts, and system developers [52]. However, as the diversity of the experts expands, it becomes more complex for communication and understanding partly because different domains utilize their own vocabulary [52] . Remedying such a problem would require the use of a common communication language that can easily be understood by all stakeholders. Despite such a need, suitable guidelines and tools to support compliance management are often lacking [13]. The lack of methodological and tool support means that the identification of compliance risks is conducted in an unstructured or semi-structured brainstorming that essentially relies on using lawyers’ imaginations. However, as lawyers are not necessarily trained as risk analysts, such an exercise often involves uncertain outcomes.

The RASEN approach enables a risk-driven compliance assessment. By risk-driven we mean that compliance requirements can be prioritized based on their risk levels or uncertainties in compliance requirements can be dealt through risk assessments. So one of the motivations behind the integrated approach is that when there is the need for such kind of risk assessment, how do you do it in the most structured manner. Figure 12 depicts the overall method for integrated risk and compliance assessment. Our aim is to bridge the gap between the compliance assessment and the risk assessment parts. To this end, we provide a structured approach for identifying and graphical modeling of compliance risks from legal or other requirements as depicted in Figure 13. The process aims at facilitating the identification of compliance risks and their documentation in a consistent and reusable fashion. As part of the process, a systematic approach for a graphical modeling of compliance risks is provided, which aims at facilitating communication among experts from different backgrounds.

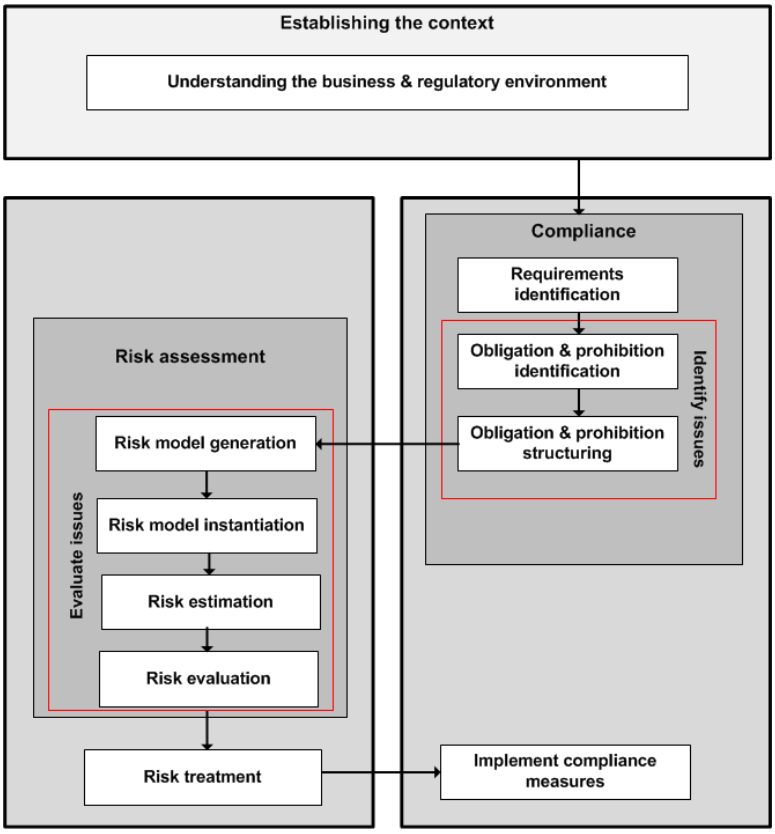

Figure 12 – Integrated risk and compliance assessment

5.2 Structuring the Identification of Compliance Risks: Support Based on Natural Language Patterns

Different international standards provide guidelines for managing compliance. Prominent among such standards are the Australian Standard on Compliance Programs [1] and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) [6]. Both the Australian Standard on Compliance Program and its COSO counterpart call for conducting compliance risk assessment, which typically involves compliance risk identification, risk estimation, risk evaluation, and risk treatment. However, neither the Australian Standard nor its COSO counterpart provide a systematic approach to identifying legal and compliance risks. Due to the lack of methodological and tool support, the compliance risk identification often involves unstructured brainstorming, with uncertain outcomes. In RASEN, we propose a five-step process for the structured identification and assessment of compliance risks. This process aims at facilitating the identification of compliance risks and their documentation in a consistent and reusable fashion. As part of the process, we provide a systematic approach for a graphical modeling of compliance risks, which aims at facilitating communication among experts from different backgrounds. The creation of graphical models can be partly automated based on the natural language patterns for regulatory requirements. Furthermore, the structuring of the compliance requirement in a template aims at simplifying the modeling of compliance risks and facilitating a potential future automated modeling. While less formal approaches are still relevant in many contexts, in a complex business environment, such systematic and structured approaches may be advisable. This section presents the structured approach for compliance risk identification. The approach consists of five main steps, as shown in Figure 13 and some of these steps contain further specific activities. The main objective of each step is described in the respective sections. A more detailed description of the structured approach is documented in [9].

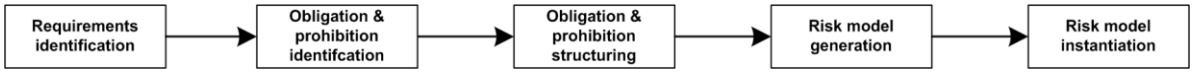

Figure 13 – Steps for structured identification of compliance risks

5.2.1 Step 1: Requirements Identification

This step involves the identification of relevant sources of requirements that should be complied with. This step is not peculiar to our approach and is an integral part of any compliance (risk) assessment approach. To identify compliance risks, initially, it is important to precisely select the relevant sources of compliance requirements. As noted above, the source of requirements could be binding, such as contracts, legal regulations, court decisions, and administrative decisions. In addition, the sources could be non-binding by nature, such as industry and organizational standards, principles of good governance, and ethical standards. Frequently, organizations voluntarily adopt to abide by such standards. In this regard, a good starting point is to use the business objectives of the entity on whose behalf the risk assessment is carried out or the target of the analysis. Once the objective of the entity or the target concerned is identified, the next step is to identify the relevant source of requirements in the area and assess whether such requirements are relevant for the actor or the target. Some relevant guiding questions for this task include: What are the relevant compliance requirements applicable to the objective pursued by the organization? Which of these requirements does the organization want to ensure compliance with? If the objective is to ensure compliance of a specific target, then the relevant question would be: What requirements might apply to the target at hand?

5.2.2 Step 2: Obligation and Prohibition Identification

Once a set of relevant sources of requirements is identified, the next step is to identify compliance requirements by making a list of obligations and prohibitions. An obligation prescribes the specific actions that an actor must undertake, and a prohibition stipulates the actions that an actor must avoid in order to ensure compliance. A guiding question for this task could be: what obligations and prohibitions are incumbent on the actor or the target at hand? Such identification could be supported by natural language patterns [26] [3] and Hohfeld's [17] legal taxonomy.

Although it is possible to define up to six different categories of natural language patterns, for our purposes we will focus only on the basic activity pattern and the modality pattern [26][3].

The first step in identifying obligations and prohibitions is a clear designation of the entity on whose behalf the risk assessment is being carried out. Often such actor is represented in the role it plays, such as bank, trader, data controller, and so forth. In using the natural language pattern terminology, this entity is annotated as the subject. According to the basic activity pattern, a compliance norm generally describes an actor (subject) performing specific actions (verb) on another actor (object) with the aim of achieving compliance to the specific compliance norm [26]. Thus, the basic activity pattern follows a "subject-verb-object (SVO) sentence structure, where the subjects come first, verbs second, and objects third" [26]. However, sometimes, the subject might only be mentioned at the beginning of the source of requirements, for example, the provision dealing with the material scope, and the subsequent provisions might not make specific reference to the subject. This is particularly the case when the source covers many actors. Thus, it is important to keep in mind such situations when using the basic activity pattern.

Once the subject and object of a compliance norm are identified, the modality pattern becomes relevant in identifying obligations and prohibitions. The modality pattern helps to identify modal verbs in a compliance norm, which determine if the specific compliance norm expresses an obligation, permission, or right of stakeholders [26]. Some of the words that express modality notations include "*may, shall, should, must, has right, has no right, may not*" [26]. This means the basic activity pattern describes subjects (who), verbs (do-what), and objects (on-whom), whereas the modality pattern determines "whether the subject of the sentence has an obligation or prohibition on the accompanying verb" [26].

[3] uses a number of normative phrases that guide the process of identification of rights or obligations. Using the natural language patterns, the authors identify different patterns where rights and obligations are expressed within the US Health Insurance Portability and Accountability Act (HIPAA) [3]. According to the authors, some of the patterns for expressing obligations in HIPPA include:

1. <actor> should <verb> …
2. <actor> should be <verb'ed> …
3. <actor> must/must be <verb'ed> …
4. <actor> will/would <verb> …
5. <actor> may not <verb> …

Although the authors do not clearly specify such a pattern for prohibition, their pattern for obligation includes a reference to terminology that is used to express prohibitions. More particularly, the reference to <*actor*> *may not* <*verb*> is to a prohibition rather than an obligation. Such a pattern and the negation of obligation patterns could help to identify prohibitions. In other words, expressions such as <*actor*> *must not* <*verb'ed*>; <*actor*> *shall not*> <*verb*>; <*actor*> *should not* <*verb*> represent prohibitions.

Although the focus of compliance risk is on obligations and prohibitions, the idea that a right of one party confers an obligation to another should not be forgotten. According to [17], a right of one party is correlated with a duty of another party. For example, in the case of data privacy rights, the right to access one's personal data confers obligations on data controllers to provide that access. This means some of the rights could be obligations of the actor on whose behalf the risk assessment is being conducted. Although the use of the natural language patterns to identify such obligations is limited, they can still provide some assistance. [3] provided a list of patterns within HIPAA where rights are expressed. These include, for example, (1) <*actor*> *may* <*verb*> and (2) <*policy*> *permits* <*actor*> *to* <*verb*> [3]. Once the actor is annotated as the subject within the basic activity pattern and the object is identified, a combination of the <object> followed by the modal verbs used to express rights can sometimes provide some help in identifying the rights that should be treated as obligations from the part of the actor (subject). This means (1) <*object*> *may* <*verb*> and (2) <*policy*> *permits* <*object*> *to* <*verb*> might sometimes impose obligation on the "actor."

It should be noted that the natural language pattern primarily involves a manual process that provides support in identifying the relevant elements in compliance norms and their modalities. However, there have been attempts to provide tool support for such manual processes. For example, [27] built on the work of [3] to facilitate automation. The authors discuss a tool named Cerno to annotate legal texts with normative phrases, discussed in [3], and then identify actors, rights, and obligations. Although their use of the tool and its accompanying process was limited to the normative phrases used in the HIPAA document, the authors claim that the tool-supported process can be re-used, with some revision, in a different domain due to its modularity [27]. According to the authors, the Cerno-based tool "facilitates recognition of relevant text fragments" and "seeks to improve the productivity, quality and consistency of the manual process" [27]. Nonetheless, in this work, our focus is on the manual support that the natural language patterns provide in identifying the subject (actor to which the rule applies), the verb (activity), the object (the target of the activity) and the modality (whether the subject has an obligation or prohibition). The patterns for identifying exceptions and preconditions can also be useful for this step but are not discussed as they introduce further complexities.

The result of this step is a list of obligations and prohibitions for the actor, including the specific reference to the article or section containing these requirements.

5.2.3 Step 3: Obligation and Prohibition Structuring

This step aims at structuring the relevant elements extracted using the basic activity and the modality patterns. Table 3 shows the template for structuring the elements identified in step above. As discussed in the next step, these elements are relevant for starting the risk assessment. Furthermore, the structuring of these elements into the template aims to facilitate the modeling of compliance risks and their potential automation.

Source of requirement	Name and/or year Section/Article number
Modality	Obligation: <actor> ***should/must/*** <verb> or Prohibition: <actor> ***should not/may not*** <verb>
Actor	<X> (subject)
Activity	Obligation: <actor> should/must***/*** <***verb***> Prohibition: <actor> should not/may not <***verb***>
Object (target)	<actor> … <verb> <***object***>

Table 3 – Template for structuring requirements

In identifying the elements in the Table, the use of the basic activity pattern and the modality pattern as discussed in step two are relevant. The subject (who), verb (what), and object (on-whom) of a requirement are identified using the basic activity pattern, and the modality of the requirement is determined with the help of the modal verbs described in the modality pattern. This means an obligation is often expressed as <actor> followed by the modal verbs such as "*should, must, must be*…" However, as noted above, the actor might not always be mentioned expressly in the compliance requirement. We have also noted that some rights conferred on other actors might result in an obligation for the subject. This also needs to be considered when using the basic pattern. Then, the <verb> in the basic pattern is the activity for both the obligations and the prohibitions.

5.2.4 Step 4: Risk Model Generation

This step involves the modeling of the relevant elements of the requirement for the compliance risk assessment. The structure in the above tables corresponds to elements of the graphical model, so that a transfer from table to model is facilitated. Thereby, the graphical model is structured based on the outputs of the analysis of requirements in previous steps. In RASEN, we use the CORAS modeling language and tool. Figure 14 has been adopted from [37] and shows the CORAS notions and their graphical representations.

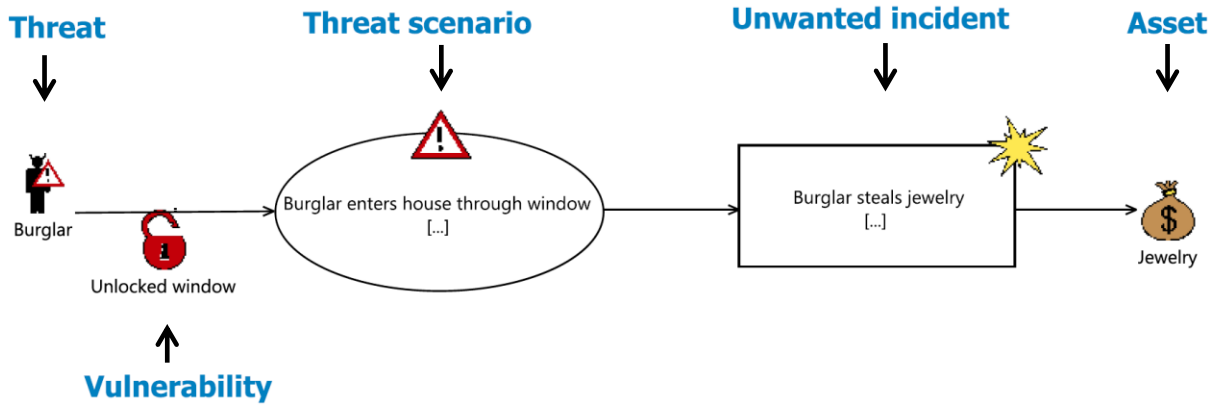

Figure 14 – CORAS notions and their graphical representations

In order to model the compliance risks, the elements documented in Table 3 can then be mapped to the above CORAS artifacts.

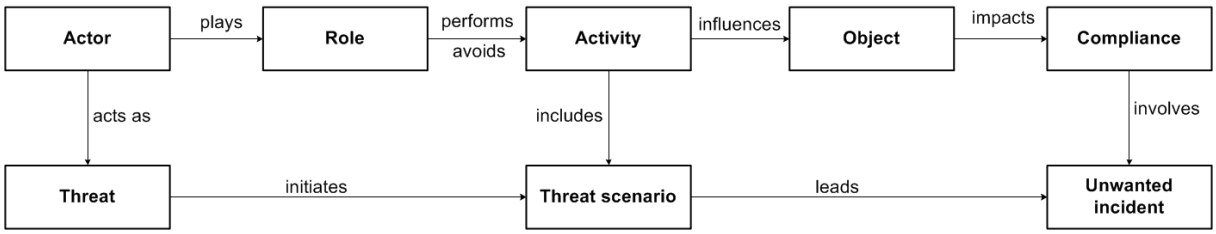

Figure 15 – Mapping compliance to the CORAS conceptual model

The mapping in Figure 15 shows a conceptual relation between the CORAS language and key normative notions used to assess compliance. This relation can be used to generate generic threat scenarios and unwanted incidents from the obligations and prohibitions. By 'generic' we mean that both the 'threat scenarios' and 'unwanted incidents' are schematically derived from the requirements as such and are generally applicable to all actors subject to these requirements. The advantage of this approach is that the model is derived directly from the requirement. At the same time, it is still "generic", so it needs to be customized before it can be used to express an identified risk. We have noted above that the lack of an existing knowledge-base in the area of compliance means that the identification of legal and compliance risks involves a substantial amount of analytical activity that, when unstructured, can be time consuming. The main goal of the schematic derivation of the threat scenarios and unwanted incidents is to reduce the effort involved in identifying legal and compliance risks. This is achieved by providing the risk analyst with such generic threat scenarios and unwanted incidents, which can be further instantiated as relevant to the specific target or entity.

The generic threat scenario is derived based on the 'verb' in the basic activity pattern discussed in step 3. As noted above, the <verb> in the basic activity pattern is the activity for both the obligations and the prohibitions. Once we have the activity (represented as a verb) identified, we can obtain the generic threat scenario by focusing on how the requirement is contravened. Where the requirement is an obligation, it is contravened when the actor fails to do the required activity, for example a failure to do mandatory work. Thus, the generic threat scenario can be schematically generated by adding the words "failure to" "verb" often followed by the <object>. If the requirement is a prohibition, the generic threat scenario is generated by adding "ing" to the "verb" and often followed by the <object>. Non-compliance then means do*ing* a prohibited action. In both cases (obligation or prohibition) the resulting non-compliance with a requirement can be seen as an unwanted incident. It might be slightly artificial to refer to a state of non-compliance as an "unwanted incident", because "incident" seems to carry the connotation of some external event in the real world. It may be the case that a state of non-compliance has no consequences, as yet. The word "incident" is fully adequate when the non-compliance has specific consequences, for example, if it is sanctioned. However, if an organization or individual values compliance, it will also consider non-compliance as a state that deviates from what is desired. Thus, the template to structure compliance requirements can be extended with two rows (threat scenario; unwanted incident) that are needed for the risk modelling.

Source of requirement	Name and/or year Section/Article number
Modality	Obligation: <actor> ***should/must/*** <verb> Prohibition: <actor> ***should not/may not*** <verb>
Actor	Subject
Activity	Obligation: <actor> should/must***/*** <***verb***> Prohibition: <actor> should not/may not <***verb***>
Target (object)	<actor> … <verb> <**object**>
Threat scenario	Contravene obligation: not do activity (what) *<failure to> <verb><object>* Contravene prohibition: do activity (what)

	<verb'ing> <object>
Unwanted incident	*<Non-compliance with> <source of requirement>*

Table 4 – CORAS-based extension of the template

As shown in Table 4, the generic threat scenario is derived by contravening the obligations and prohibitions. Similarly, the generic unwanted incident is derived by negating the source of the requirement. This approach of negating a certain element to obtain a threat is a commonly used technique in many risk assessment approaches. For example, STRIDE, a threat taxonomy which is used to identify security threats, is an acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege [9]. These threats are the negation of the main security properties—namely, confidentiality, integrity, availability, authentication, authorization, and non-repudiation [9]. Similarly, KAOS, a goal-oriented requirements analysis framework, provides a goal-based threat modeling approach based on the negation of the goals (anti-goals) as threats [8].

Table 4 can then be modelled in CORAS as shown in Figure 16. As noted above, the structuring of the elements of the requirement into the template aims to facilitate the modeling of compliance risks and their potential automation. Given that the template provides all the components, the modeling in CORAS becomes straightforward.

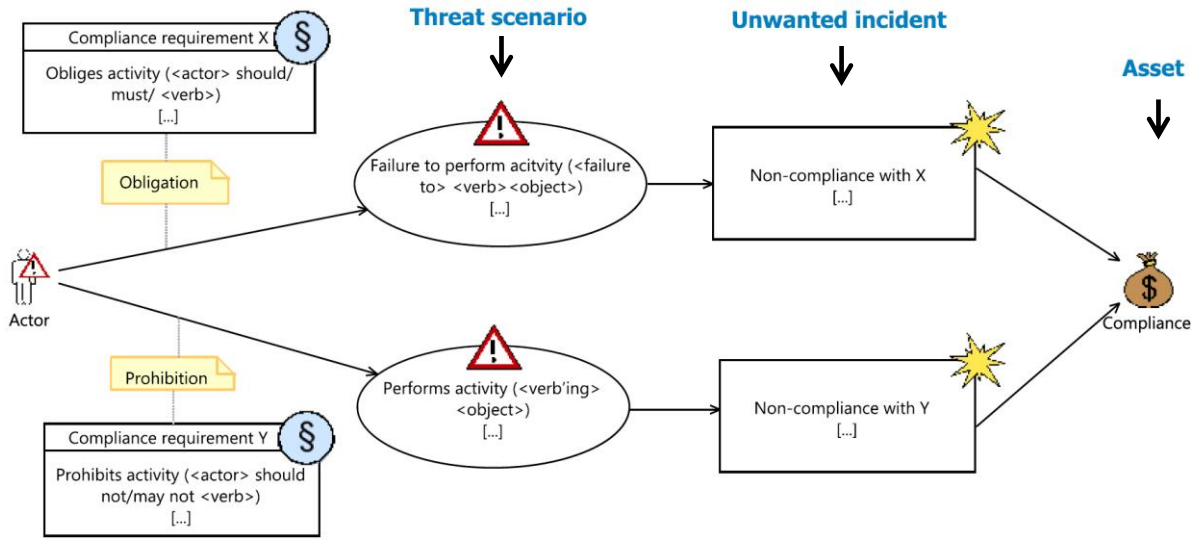

Figure 16 – Modeling compliance threat in CORAS

The results of this step are a generic compliance risk modeled in CORAS. The creation of such generic risk models from regulatory instruments has many advantages. First, it facilitates reusability. The fact that such risks are generic and based-on the requirements means that there is no need to start from scratch every time there are changes in an organization or system. These generic risks can still be relevant so far as the requirements remain valid. Second, the use of generic threats clears the way for the creation of databases containing generic risks relevant for specific regulatory instruments. For example, it is possible to populate a database with the generic threats of a specific regulatory instrument, which can be instantiated by individual actors subject to that instrument. In addition, through time, such database can be filled with relevant causes for generic threats (such vulnerabilities and other information), gearing towards having databases analogous to CAPEC for the purposes of compliance risk assessment.

5.2.5 Step 5: Risk Model Instantiation

As shown above, step 4 ends with generic compliance threats and unwanted incidents that can be applicable to any actor or target which is subject to the same regulatory requirement. For example, the generic threat scenario "*crossing the street while the traffic light is red*" derived from the Traffic Roads Act is equally applicable to all actors regardless of their attentiveness, visual impairment, or whether the street is busy with traffic. Such factors are relevant because they will affect the likelihood of "crossing the street" and its consequences, which are essential in determining the risk levels. Given that every actor has its own goals and values and operates under its own unique environment with different priorities and resources, such generic threats are not representative of that particular circumstance within the entity or target which is the focus of the risk assessment. Therefore they need to be instantiated. Similarly, the unwanted incident, which is described as "non-compliance with Traffic Roads Act Art.25", might be too generic to be understood and would need to be specified further. This step aims at instantiating these two aspects.

5.1. Identifying Triggers

The first activity in this step is to identify the triggers for the respective generic compliance threats. Doing so is important because different factual circumstances could give rise to the failure to perform the obligatory activity or to the performance of the prohibited activity. In addition, the triggers are what make the risk assessment specific to the actor or target under analysis. Therefore, all possible causes and triggers of the threat can be identified by asking a relevant guiding question, such as:

- How can the given scenario occur?
- What could lead the actor to contravene the obligation or prohibition?
- What control measures are in place to prevent the scenario from occurring? What could cause their failure?

Taking generic risks as a starting point and instantiating them is also common in well-established risk analysis techniques. For example, the STRIDE threat modeling process has nine high-level steps [9]. A particular resemblance to our approach of instantiation can be found in steps six and seven of the STRIDE threat modeling process. In step six, the main objective is to identify security threat types based on the generic threats (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) [9]. As mentioned above, these threats are the negation of the main security properties. In step seven, these generic STRIDE categories are used to identify the preconditions for each STRIDE threat category using the threat tree pattern [9]. The STRIDE-based generic threats are referred to as *root threats* and the preconditions as *concrete threats* [9]. The approach followed in fault tree-based risk analysis techniques is also similar to this in that the *root node* describes a high-level attack which is further decomposed in lower-level attack branches or *leaf nodes* [9].

Our approach of deriving the generic compliance threat models described in the step above and their instantiation in this step are comparable to steps 6 and 7 in the STRIDE threat modeling process. The generic compliance threats derived schematically are comparable to the root threats in STRIDE (high-level braches or root node in fault-tree) and the triggers are comparable to the concrete threats (lower-level attack branches or leaf node in fault-tree). This means our approach can easily be integrated within the tree-based or STRIDE risk analysis frameworks. Nevertheless, our framework can be performed independent of those.

One drawback of our approach could be the lack of reusable information as analogous to what is provided by STRIDE. STRIDE comes with an extensive, reusable knowledge base (i.e., the threat tree patterns), which provides significant support in identifying the concrete threats [9]. Databases such as CAPEC could also be used to complement the identification of the relevant preconditions. This means there is existing reusable information available that facilitates the identification of the preconditions (concrete threats) for the root threats. From a compliance perspective, the lack of such a reusable knowledge base could be a challenge. This means that finding the triggers would still be a manual exercise and dependent on the analytical skills of the participants. However, the use of the structured guiding questions identified above could mitigate some of the challenges. Furthermore, at least in some areas there is a reusable knowledge base that could be used as triggers. For example, the ENISA [10] cloud vulnerability list provides a list of vulnerabilities introduced by the cloud, including some that affect compliance. And in assessing compliance risks arising from the adoption of cloud services, such a list could be of relevance in providing the triggers. Similarly, in the areas of data

privacy, the threat pattern catalogues discussed in [9] could be useful to consider. Furthermore, in the long run, the idea of establishing compliance-focused and CAPEC-like databases with vulnerabilities and threats, if realized, would be a big step forward in mitigating such a challenge.

5.2. Instantiate Unwanted Incidents

This step aims at instantiating the generic unwanted incidents in terms of consequences. More particularly, it aims at investigating what values are reduced or endangered by not complying with the specific requirement. In other words, this step enables the consideration of sanctions and other consequences of non-compliance with the obligations and prohibitions. Similarly, there might be other requirements or conditions that need to be considered in combination with the requirement under consideration or with its non-compliance. At least from the business perspective, such instantiation could also be relevant for communicating the results of the risk assessment to other stakeholders. This is because the generic unwanted incident “non-compliance with Article X or Y” might not be specific enough to understand the implications. Thus, it would be relevant to instantiate such generic incidents further, for example, in terms of the regulatory penalties, or potential prosecution of management, or potential monetary or customer loss.

5.3 RASEN to Support Cloud Sourcing

The RASEN methodology has been applied in a complex industrial case study. The risk assessment in the case study focuses on the compliance risks of a complex ICT system and services that handle confidential information. The motivation for the risk analysis is to evaluate the compliance risks associated with the potential use of a cloud service. The context and evaluations results of the case study are detailed in another upcoming work [12]. One of the lessons learned during the application of the case study was that ‘risk is the same’ for the cloud and non-cloud scenarios. This means there is no need to develop a different methodology for cloud scenarios. Nevertheless, in this section, attention is paid to supporting the RASEN methodology with existing, reusable knowledge in the adoption of cloud services. The approach helps to consider the main legal compliance issues in adopting cloud services and their potential remedies. This is achieved in three ways. First, based on literature review, we identify high level regulatory requirements that are relevant, from the customer’s view point, in the adoption of cloud services. Second, these high-level regulatory requirements are mapped to the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). This involves identifying a control domain from the CSA CCM that can help address the specific compliance concern. Furthermore, we support the identification of triggers in the RASEN methodology with the ENISA vulnerability list [10].

5.3.1 High-level Compliance Requirements Relevant During Cloud Sourcing

As part of this task, we identify generally relevant compliance requirements that need to be considered during cloud outsourcing. As noted above, the identification of the regulatory requirements is based on literature review and experience regarding which compliance issues are of most concern to cloud users although these requirements are also relevant from the cloud provider’s point of view. However, it is important to note that the category of regulatory requirements is not exhaustive. This means depending on the type of cloud service sought and the jurisdiction of the cloud user, there might be requirements which are not covered in such category. Thus, one has to note that the list is just a starting point and can be grown with newly enacted rules and rules that are not foreseen in this report. Furthermore, the categorization is not exclusive to each other – meaning that certain requirements might fall in more than one category. It should also be noted that the focus of the requirements is on private cloud customers as opposed to use of cloud by public entities, which could raise additional compliance issues. The identification of the rules is based on the characteristics that the cloud customer cedes control to the CP on a number of issues, which may affect compliance.

Data privacy rules – this category concerns the protection of personally identifiable information (personal data as it is referred to in the EU). Personal identifiable information is information that can be associated to a natural person. Data privacy rules are considered as main source of concern in adopting cloud services. According to a European Commission study [5] the most important concerns in cloud adoption are “data protection compliance, information security, and jurisdiction/enforcement.” Similarly, ENISA has put data protection compliance as one of the top risks of cloud computing [10]. Some of the data privacy rules around the globe include the European Data Protection Directive (now

under reform), the Canadian Digital Privacy Act, and the Australian Privacy Amendment Bill that took effect in March 2014. However, often a mistake is made in considering data privacy as similar to information security. Although information security is an essential part of data privacy rules, it is not the only aspect. Hence, we further categorize into different aspects of data privacy. The outsourced nature of the cloud and the inherent loss of control that goes along with using cloud computing services require that data be carefully controlled. No detailed guidance is aimed regarding whether the cloud provider is considered a data processor or data controller.

Data security – this is similar to information security. This can further be categorized into technical and organizational measures. Technical measures include the classic information security aspects such as '*availability'* —which includes measures against the accidental or unlawful destruction or loss of data; '*integrity'*—which includes measures against alteration of personal data and *'confidentiality*' that includes measures against unauthorized disclosure of, or access to, personal data. The use of technical measures such as anonymization and pseudonymization falls under such measures. In this regard, the inherent loss of control over data or IT resources resulting from the move to the cloud opens for new vulnerabilities in the technical measures to be implemented by the cloud customer.

Organizational measures include adoption and implementation of internal policies on data protection practices. This includes conducting risk assessments and providing appropriate trainings to employees. Organizational measures also include ensuring compliance with the data protection rules where processing is carried out by a third party. This includes entering into contractual agreements with the third party and ensuring that processing is conducted in compliance with applicable data privacy rules.

Data security is at the forefront of the concerns in using cloud services, particularly public clouds. The physical impediments to security threat in the traditional IT model have vanished with the emergence of cloud and anyone connected to the Internet can be a threat to security measures deployed anywhere in the cloud. Such security threats can emanate from the cloud users themselves in the form of spying and interfering in each other's activities or from third party insiders (such as the provider's employees' and sub-contractors). The insider threat can result in abuse or sabotage of the data for purposes other than originally intended. In addition, the cloud has taken the data closer to attacks by third party outsiders (with no connection to the provider) as the only barrier between data in the cloud and any person connected to the Internet is often a simple password and username.

Overall, the security challenges in relation to the cloud environment emanates from lack of control on the provider's resources, increased exposure of internal infrastructure via new technologies/interfaces, insufficient adaptation of application/ platform security and development lifecycle, unclear ownership of security tasks and lack of cloud specific security standards [7]. This implies that both cloud providers as well as cloud users have to be aware of the existence of such risks and take appropriate measures to address these risks.

Location of data and data transfer rules – some data privacy rules also impose location-based restrictions. For example, the European Data Protection Directive 95/46/EC has put in place the general principle that the transfer of personal data to any country outside the European Economic Area (EEA) is prohibited unless that third country ensures an adequate level of privacy protection. This obviously has particular implications as cloud computing will in most cases involve the international transfer of personal data. In addition to the places of storage and processing, attention should also be paid to the location of the people accessing and processing data. The controller will therefore be required to comply with the data protection regulation related to data transfer. Also, the use of servers or providers outside the territory where the data is collected opens for access by foreign law enforcement authorities as a potential threat in cloud scenarios. Furthermore, each jurisdiction has unique restrictions on, and requirements providing for, law enforcement access to data. Thus, the customer should pay attention to information available from the provider about the jurisdictions in which data may be stored and processed and evaluate any risks resulting from the jurisdictions which may apply.

Data subject rights – most data privacy rules provide rights to data subject such as the right of access to one's personal data, the right to object to the processing of their personal data and to rectify inaccurate data. Under the ongoing EU reform, data subjects are also given the right to obtain deletion of their data. In a cloud scenario, given the data is going to be processed in the providers resources means that, in some cases, arrangements should be made to enable the data subjects exercise their

rights. Another such right could be data portability. Data portability relates to the ability to transmit personal data and other information from one service to another one. The undergoing reform on data protection extends this concept also to include the right to obtain a copy of their personal data from the controller “in a structured and commonly used format” that enables its further use provided that the data is processed by electronic means. However, it has to be noted that data portability is not a legal right for cloud users as such, meaning that it is not clear if corporate customers can claim such right to move data. This notwithstanding, customers looking for cloud services to store or process personal data should consider the providers readiness to facilitate such rights of the data subject when necessary.

Breach notification requirements – This generic category of rules includes requirements for the notification of breaches affecting a network, service or a data. Breach notification requirements are often affected by the use of cloud services because the cloud customer might not have information to breaches occurring in the cloud providers infrastructure or services. Similarly, the cloud provider might not be aware that the customer has obligation to report such breaches unless specifically instructed to do so. It has to be noted that the involvement of the cloud provider does not reduce any of the conditions regarding, timeframe, and content to be complied with. Therefore, it is recommended that the obligation of the provider to notify the customer immediately if a breach occurs be set out in a contract. Nevertheless, given that many cloud providers offer non-negotiable standard terms of service, it may be difficult to negotiate such notifications into the contracts for many controllers, particularly SMEs. In fact, at least in the EU, recent legislative initiatives impose such an obligation on the cloud provider. For example, according to Article 31(2) of the draft General data protection Regulation processors are required to inform and alert the controller of any personal data breach.

Retention rules – govern the retention of data or documents for a specified period of time. This includes the retention of usage data of certain services for national security reasons, or the retention of personal (health related) data or record for tax related purposes or the retention of employee related data. Although the use of cloud services is not a major concern for these rules, the cloud providers need to be informed of such obligation so that it facilitates their maintenance during the life of the cloud contract and after.

Documentation and archiving rules – addresses obligations of the cloud customer to keep a documentation of organization’s ICT systems, documentation of risk assessment results, documentation of auditing results, documentation of discrepancies and breaches and so forth. The fact that the cloud provider is entrusted with most of control on these aspects means such obligation might give rise to compliance issues.

Auditing rules – impose obligations on the cloud customer to allow regulatory authorities to conduct audits for compliance with certain requirements. This means, the cloud customer should take appropriate measures in ensuring that the cloud provider will cooperate when such auditing arises. However, such requirements are often fulfilled also by requesting third party certifications from the cloud provider.

Data ownership and illegality of content – The issues related to intellectual property rights arise on several levels when considering a cloud environment. First, one shall note that when data is uploaded, exchanged, stored or more generally processed in the cloud, the Cloud Service Provider (CSP) may create items protected under intellectual property rights, such as in particular copyright-protected works, databases or computer programs. In such context, it is of particular importance to contractually address the issues related to the existing IP protected materials and the status of newly created items (such as ownership, transfer or licensing of rights, what happens after termination of the relationship, etc.). This also includes pre-contractual negotiations which may give rise to joint results which can be the object of intellectual property rights (for example, techniques to better handle data) [10]. Therefore, measures should be taken to determine who will own these rights prior to engaging in cloud computing activities, and further determine the use that the parties can make of the objects of such rights.

Secondly, cloud computing platforms can be used to store and exchange illegal content, and in particular content infringing intellectual property rights (namely copyright-related protected materials). Such contents which are legal under the jurisdiction of the cloud customer might not be legal in the jurisdiction it is hosted. This means, such data might be subject to law enforcement actions such as seize and access. In general, liability lies with the person who infringes the intellectual property rights

(primary liability). However, in certain circumstances, the question of the liability of intermediaries, such as hosts, may arise (secondary liability).

Trade secrets are also an important tool for business and research bodies. It is consequently important to protect such valuable information. However, trade secrets are currently not protected by formal intellectual property rights under European level and are only relatively weakly protected by national law against misappropriation by third parties in almost all EU Member States. Indeed, there currently exists no common legal framework in the EU on the protection of trade secrets, and thus no uniform definition of "trade secrets" exists within the EU. As a result, despite the weak legal framework, it is important to put in place all necessary measures through contractual clauses in order to address the issues related to the protection of trade secrets and the misappropriation of such information through cloud computing services

E-discovery rules – address request by government agencies to access a data or infrastructure in their role as law enforcement. This covers requests directed at the cloud provider or requests directed at another cloud customer not only for 'public security' reasons but also for economic espionage in the domestic interest. Although such threats are often associated with undemocratic countries, even Western Democracies have laws allowing government authorities to access records. Prominent examples are the USA PATRIOT Act 2001 and UK Regulation of Investigatory Powers Act 2000 that allows for access of electronic documents. This means the cloud user needs to consider what should the cloud provider do before complying with such requirements and pro-active assessment of the leniency of such rules in the jurisdictions where the cloud provider might be subject. These aspects need to be evaluated. Furthermore, the cloud customer itself could be subject to such request by government authorities to provide access to the infrastructure or data. This includes making certain information available within a certain period of time. Thus, the forensic readiness of the cloud provider should be assessed. Furthermore, the cloud provider himself or a third party using the services could be subject to civil suits or subpoenas, which could in turn affect other cloud customers.

Contractual issues – this constitutes some of the contractual issues in procuring cloud services that need to be considered because they might also affect compliance issues.

Liability and warranties – most CSPs seek to exclude liability and offer no warranty for lost data or damages resulting to the customer. Although there are more warranty options in the case of paid services, the warranties are often limited to nominal amounts or service credits. Some disclaimers of warranty even attempt to remove liability for infringement of third-party intellectual property by the CSP. The validity of such disclaimers might depend on the parties involved (whether it is business to business or business to consumer contracts). Despite this, customers using the cloud particularly to store or process 'sensitive' personal data should take precautionary approach than relying on the reactive provisions. This advice is all the poignant given that it is also not easy to identify the party responsible in a case of breach.

Change of terms – it is common that many terms offered by CSPs allow for the right to modify the terms of the agreement unilaterally. Depending on the agreement, the terms allowing for this modification may be drafted broadly and provide cloud consumers with little ability to object or even evaluate changes to the service. CSP's often retain the right to unilaterally amend specific terms of the contract for a variety of reasons. Thus, arrangements should be made to the effect that the cloud customer becomes aware of such changes the least or even approve such changes.

Subcontracting – one potential threat in a cloud may arise from the customer not knowing that chain processing is taking place involving multiple sub-contractors. Such chain of actors may include software and storage providers, ISPs, or other network providers located in different countries. Although the term "partners" is often used in agreements, infrastructure and other providers are not necessarily under the same corporate or organizational umbrella. Their association or contractual relationship is often limited to individual agreements with the CSP. In fact some EU countries prohibit the CSP from subcontracting to a third party unless the customer gives authorization to do so. Thus, contractual measures to address such issues should be put in place or request the cloud provider to provide an overview of the actors that are involved in the provision of the service.

Choice of law or jurisdiction – as CSPs generally operate across multiple jurisdictions and therefore make attempts to limit their risk of being draw into judicial proceedings in all the locations they operate. Thus, the terms and conditions of most CSPs stipulate that the application of a law and a court of jurisdiction in which they have principal business place. Such terms would then drag the cloud

customer to litigate in a foreign jurisdiction where there is contract disputed related with the provision of cloud services. Such terms and conditions need to be reviewed carefully by cloud customers.

Data portability – the ability of cloud users to move data between providers or cloud services or else to pull-back the data where the relationship with the provider is terminated. From one service to another service is considered a serious obstacle to further development and use of cloud computing. Portability challenges may come from different sources. On the one hand, cloud consumers may have a limited ability to move to a new provider as a result of reliance on a specific CSP. This can be attributed to lack of standardized data formats or service interfaces. Cloud consumers may become dependent on one CSP's proprietary technology to the point that moving to another CSP would negatively impact business processes. In the case of Software as a Service (SaaS) users, it may be difficult for a cloud consumer to find a comparable service. On the other hand, if the CSP uses a proprietary format, making the cloud consumer's data unusable with another provider, options from migrating to another service are also limited.

In addition to practical or technical barriers, the contract may also provide limits on the cloud consumer's ability to freely move data. For example, removal of the cloud customer's data may be subject to what is deemed a "data hostage clause." Data hostage clauses often require that the cloud consumer pay all debts and/or settle all disputes before removing data. If the clause requires that all disputes be settled before data can be moved to another service, the cloud consumer has little choice to but to make payment, even if they have a legitimate dispute.

Termination of contract – when data is being stored on the cloud, the terms of the contract will define the rights and liabilities of the parties when the agreement ends. Even as early as the pre-contractual phase, the cloud consumer must consider the eventual dissolution or termination of the cloud computing service. Whether the termination is a result of a contract term ending, sale or merger of the provider, consolidation, bankruptcy of the service, or even non-performance or breach of contract by the CSP, the contract should provide the terms necessary to make the smoothest transition of data back in-house or to another CSP. Vague or missing terms of cloud computing agreements might make a smooth transition, or any transition, difficult.

5.3.2 The Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)

The CSA CCM covers the following control domains for cloud computing services, which are also coded.

1. Application & Interface Security (AIS)
2. Audit Assurance & Compliance (AAC)
3. Business Continuity Mgmt & Op Resilience (BCR)
4. Change Control & Configuration Management(CCC)
5. Data Security & Information Lifecycle Mgmt (DSI)
6. Datacenter Security (DSC)
7. Encryption & Key Management (EKM)
8. Governance & Risk Management (GRM)
9. Human Resources Security (HRS)
10. Identity & Access Management (IAM)
11. Infrastructure & Virtualization (IVS)
12. Interoperability & Portability (IPY))
13. Mobile Security (MOS)
14. Sec. Incident Mgmt, E-Disc & Cloud Forensics (SEF)
15. Supply Chain Mgmt, Transparency & Accountability (STA)
16. Threat & Vulnerability Management (TVM)

5.3.3 Mapping High-Level Compliance Requirements to the CSA CCM

In this section we map the main regulatory rules that affect compliance in using cloud services with the CSA CCM so that cloud users are able to identify the relevant category of regulatory rules applicable to them and their potential countermeasures. Again, the aim is not to be exhaustive and other measures also need to be considered. The objective is rather to try and highlight the relevant control domain and the most relevant control measure for the specific category. In fact the CSA CCM also

contains mapping of the measures to some regulatory requirements such as the US HIPPA, the US Family Educational Rights and Privacy Act (FERPA), and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and other jurisdictions such as BSI Germany, Mexico's Federal Law on Protection of Personal Data Held by Private Parties and some rules from Mexico. It also includes a mapping to the European Data Protection Directive. Thus, for actors dealing with these specific regulatory requirements, they are better served by the mapping in the CCM. Although such mapping is generally relevant for actors from other jurisdictions, it is too specific and jurisdiction dependent. Thus, our approach categorizes the requirements into groups and describes the general characteristics of such requirements. This would enable any actor operating in any jurisdiction to identify the relevant rules which falls under the specific category. Furthermore, the CCM focuses on data protection requirements in particular. One of the rationales for mapping is that some cloud users might only be concerned about data privacy rules whereas others might be concerned only about IP right issues, in which case they look at the relevant category of measures for their concerns. Then the mapping to the CSA CCM can be used to include a contractual provision to address the relevant concern or to evaluate whether the terms of conditions of the provider address that specific concern. In case of the latter, the cloud users might take measures to address such concerns themselves. This notwithstanding, as noted above, not all of the legal issues raised in this guide will be relevant to each cloud computing service. For example, some issues relating to the protection of information may be less important where the provider is not holding or accessing the cloud user's data. Thus, cloud users should therefore always carefully review and obtain all necessary legal advice on the specific terms to use

Second, the mapping of a control measure to a specific category of regulatory issues does not mean that that control measure is the most effective measure that could address the compliance issue. This means other measures might need to be considered as additional or independent of the control measure highlighted in this section. Thus, this mapping only aims to assist in highlighting the main regulatory issues and their potential remedies that should be considered in adopting cloud services.

Category	Sub-category	RASEN mapping to CCM
Data privacy rules		AIS, BCR, CCC, DSI, DCS, EKM, HRS, GRM, IAM, IVS, STA, TVM
	Data security – technical measures	BCR-03, BCR-05, BCR-06, BCR-07, DSI-03, DSI, DCS-02, DCS-03
	Data security – organizational measures	AIS-04, BCR-03, BCR-10, BCR-11, CCC-03, DSI-06, CCC-03, CC-04, CCC-05, DSI-04, EKM-02, EKM-03, EKM-04, GRM-06, GRM-07
	Location of data and data transfer rules	DSI-02, AIS-04, DSI-01, DCS-03, DCS-04, IVS-13
	Data subjects rights	AIS-02, IAM-10, IAM-11
	Secondary data usage	DSI-05, DSI-07
Breach notification rules		SEF-03, IVS-01, SEF-01, SEF-02, SEF-05, SEF-05, STA-02, STA-05
Retention rules		BCR-11, GRM-02
Audit rules		AAC-01, AAC-02, AAC-03, GRM-01, STA-04, STA-05
Documentation and archiving rules		BRC-04, BCR-11, DSI
	Documentation of organizational overview	BRC-04,BRC-09, DSI-02, DSI-06, DCS-01, HRS-07
	Documentation of risk assessment results	GRM-02, GRM-04, GRM-08, GRM-10, GRM-11

	Documentation of auditing results	STA-04, STA-05
	Documentation and discrepancies and breaches	SEF-02, SEF-05
Data ownership and legality issues	Use of data by the cloud provider and creation of derivative works	CCC-01, IAM-06
	Legality of the content in the host jurisdiction	SEF-01
E-Discovery rules	Compliance by the cloud user to e-discovery requests	IVS-01, SEF-01, SEF-05
	Compliance by the cloud provider to e-discovery requests	SEF-05
Contractual issues	Liability and indemnity	STA-07
	Termination of contract	HRS-01, IAM-11
	Subcontracting	CCC-01, CCC-02, DCS-04, HRS-02, HRS-07, STA-05, STA-06, STA-009
	Portability	IPY-01, IPY-02, IPY-03, IPY-04, IPY-05
	Change of terms at the discretion of the provider	CCC-01, CCC-02, CCC-03,CCC-05, STA-03

Table 5 – Mapping high-level compliance requirements relevant for cloud outsourcing to the CSA CCM

5.3.4 The ENISA Cloud Vulnerability as Input in Cloud Compliance Risk Assessments based on RASEN

In the above section, we have demonstrated that the CSA CCM can be used in treating risks (it can be used independent of the RASEN method for evaluating the cloud service in light of the relevant compliance requirements applicable to the cloud user). This means that when using the RASEN method, the CSA CCM can be used at treating the relevant risks. Another re-usable knowledge that can support our method is the ENISA cloud vulnerability list. Given that the triggers that the causes that could lead to the generic threat scenario, then the vulnerabilities listed in the ENISA document [10] could provide input to this step. This means once the relevant compliance requirement is structured in the template and then the generic CORAS model is generated, the ENISA cloud vulnerability list can be used to select vulnerabilities as triggers that could lead to non-compliance. Furthermore, the ENISA Cloud Security Online Tool [53] can support the risk estimation and evaluation steps when the client is an SME (Small and Medium Sized Enterprise). The tool provides a mechanism to answer some questions and then gives the risk estimation of some issues in the adoption of cloud services.

5.3.5 Supporting RASEN Methodology Using the ENISA Vulnerability List and the CSA CCM during Cloud Sourcing

The high-level compliance requirements, the ENISA vulnerability list, the CSA CCM and its mapping with the high-level regulatory can then be integrated into the RASEN method to support compliance assessment during cloud sourcing. Figure 17 shows the RASEN method supported by the three artifacts.

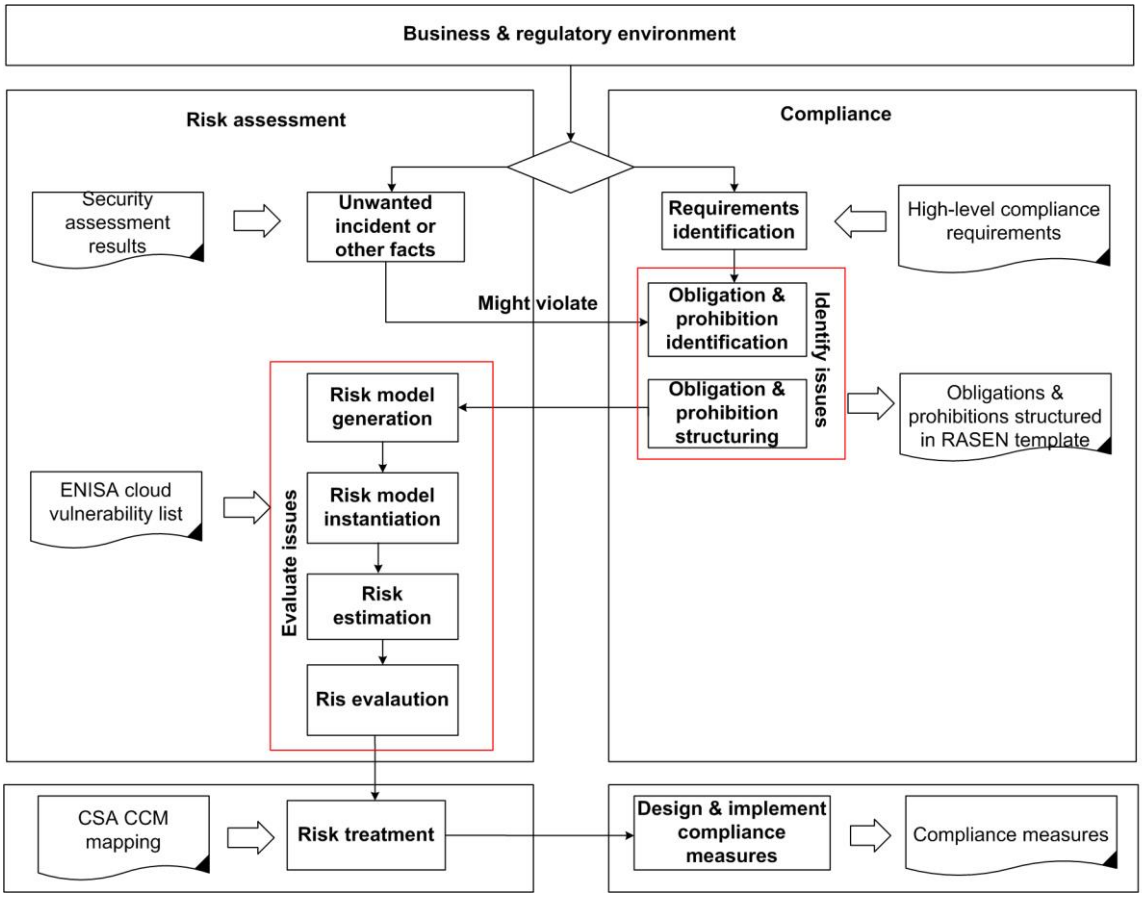

Figure 17 – Supporting RASEN methodology using the ENISA vulnerability list and the CSA CCM during cloud sourcing

5.4 Evaluating RASEN in Light of Best Practices

The RASEN method has been applied in a complex industrial case study. The case provider operates an ICT system and services that handle confidential information, including financial and personal data. The security of this system is crucial as security breaches could potentially have a negative financial impact on the customers as well as damaging the reputation of the case provider. Also, the ICT system constitutes an important infrastructure that is also used to manage electronic payment transactions. As such, it is subject to strict laws and regulations to ensure that availability of the system and to protect sensitive information of the users.

The main aim of the case study was to evaluate the utility of and understand the challenges of using the RASEN method in practice. The context and evaluation results of the case study are detailed in another upcoming work [12]. In summary, our objective in the case study was twofold. First, to employ the RASEN method in conducting compliance risk assessment in a concrete industrial case and evaluate its utility in practice. Second and related to the first was the intention to examine where the RASEN approach stands in light of current risk and compliance assessment practices. To this end, the case study consisted of a series of meetings with the partners from the industrial case provider between June 2014 and June 2015. Participants to the risk assessment included two risk analysis experts, a technical expert with the knowledge of the IT system under consideration, two legal researchers, the legal counsel, the head of compliance and the risk manager of the case provider.

The focus of the first among a series of meetings was on defining the context and scope of the compliance risks assessment. This meeting identified the risk assessment to focus on evaluating the compliance risks associated with the potential change in the business, particularly the IT environment. It was considering moving some of the components of the ICT system into the cloud. This was

envisaged to have consequences both for IT security and for legal compliance, due to regulatory limitations on the use of cloud computing. In preparation to the meeting a consultation was made with the relevant regulatory authority on the area and relevant compliance sources were identified. This was followed by a series of meetings with the above-mentioned participants to identify and evaluate compliance risks using the structured approach. As part of this task, compliance risks relevant to the cloud scenario were identified using the structured approach and documented in CORAS. The last two meetings were focused on evaluating the results found by employing the structured approach. Interviews, structured discussion and questionnaires are used to collect empirical data about the utility of the structured approach. We also use our experiences in the case study to provide perspectives of the empirical data gathered.

The main focus of our evaluation is the structured identification of compliance risk and the graphical modelling. The former involves the steps 2 through 5 of the structured method. The second aspect evaluates the graphical modelling and whether transition from normative statements (obligations or prohibitions) to graphical risk models is systematic enough. The evaluation is conducted in comparison to an alternative approach that treats compliance and risk assessment separately. More concretely, we use the framework currently in place at the case study provider (hereinafter the alternative approach), which is based on best practices, as a basis for our evaluation. The evaluation is based on the hypotheses defined below. Based on these scenarios, we are interested in learning the potential benefits and challenges in using the integrate method more generally and compared to the alternative in particular.

The main hypothesis is: *the integrated method may provide better input to decision making than the alternative*. This can be further decomposed into the following sub-hypotheses.

Sub-hypothesis 1	The integrated method enables a better structuring in the identification of and prioritization of compliance risks and may yield reusable risks than the alternative
Sub-hypothesis 2	The graphical modelling facilitates communication during and after the risk assessment
Sub-hypothesis 3	The costs of using the integrated method is, in the long run, lower than the value of the benefits from its use

Table 6 – Hypotheses

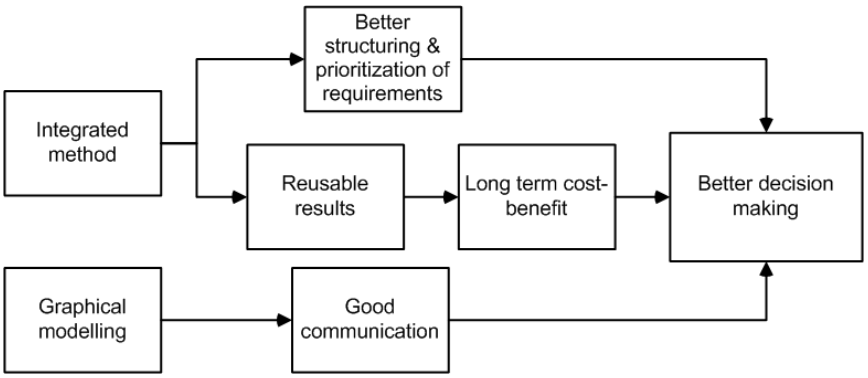

Figure 18 – Cause-and-effect relationship

Figure 18 shows the cause-and-effect relationship between the main hypothesis and the sub-hypotheses. While this case study was carried out in a business environment, with realistic issues and access to relevant expertise, it nevertheless needs to be acknowledged that there are some limitations in what can be concluded from a limited study like this. In particular, this was the first attempt to use the approach in a large-scale case. Moreover, to some degree the method was still being refined during the case study, in order to take into account how the approach worked in practice. Last not

least, it is challenging to compare the result of the case study with an alternative approach that does not involve our method. Despite these limitations, the realism of the case provided valuable insight into the potential of the approach in a practical business environment.

5.4.1 Evaluation Results

This section presents evaluation results based on the hypotheses defined above. For each hypothesis, we have defined relevant question. The following questions are asked for evaluating sub-hypothesis 1.

- What are the potential benefits of the integrated approach? Was it easy to follow and understand the steps and their intended outputs? What improvement does the method add to the current framework? What are the weaknesses of the structured approach in light of the current framework?

By providing relevant guidance in carrying out the relevant risk identification steps in a suitable order, the approach is considered to add focus and facilitate documentation of results in a consistent way. This is achieved by limiting the focus of the discussion to a specific generic threat at a time and providing a clear guidance in terms of the relevant inputs and outputs of each step. This simplifies the tasks of both the participants and the person in charge of documenting the risks. As one of the participants commented, the steps in the method are “very easy to follow”. More particularly, it is indicated that the integrated method allows “consistent structuring of compliance risks in a way that is easy to both achieve and understand.” Such structuring also facilitates the use of existing knowledge base. In the case study, the ENISA [10] Cloud vulnerability list was useful in identifying relevant triggers leading to the generic threat scenarios. The use of such information base is relevant because it enabled the inclusion of triggers that were not identified by the participants. The participants were initially asked to identify all relevant triggers to a specific generic threat and then their attention is drawn to selected vulnerabilities from the ENISA list [10]. In most cases, the participants agreed that some of the vulnerabilities are applicable to their case and have been documented accordingly. However, trying to structure and model all relevant obligations and prohibitions as discussed in steps 3 and 4 could be challenging at times, underlining the need for some selection where some could be dealt with less formal assessment whereas others could be dealt using the structured approach. In our case, we relied mainly on the concerns raised by the regulatory authority. Yet the selection might not always be an easy exercise and could be something for a future work.

The current framework at the case study provider is similar to the best practice described above. It constitutes predominantly risk management and compliance process working separately. As part of the compliance assessment, compliance measures described in standards with a focus on compliance requirement that are relevant for the case provider are implemented into business procedures and policies. This is corroborated with compliance testing. This means that the current framework does not address risks resulting from regulatory requirements as such. In other words, compliance is not risk-driven, meaning that the compliance measures are implemented without having regard to the risk implications of the specific requirements. As noted above, a risk-driven compliance enables to focus the compliance resources on the areas that are most likely to cause concern. Similarly, the risk-based compliance could improve the compliance testing currently in place in that the testing would focus on high-risk areas. Furthermore, the risk-based approach and the documentation could facilitate auditing and certification processes that the company undergoes continuously, as it is possible to produce well-structured records.

In some context, the case provider conducts compliance risk assessment as part of technical or operational risk assessments. This approach can be referred as a fact-centered identification of risks. From a compliance perspective, the focus of such risk assessment is on the legal or contractual consequences of technical breach or operational risks (e.g. service interruption). Although this approach adds a risk perspective to compliance, its significance is limited for the following reasons. First, it has limited support when there is uncertainty regarding the legal or contractual consequences itself. This often creates subjectivity in the assessment of the consequences owing to the risk appetite of the individuals. As indicated by the compliance manager, people’s appetite for risk varies significantly and thus decisions are made based on such subjective assessments. This is partly because of the lack of a formalized approach to assess compliance risks as such. Thus, it has been indicated that the integrated approach would reduce the individual’s appetite for risks and introduce

some level of objectivity in assessing the consequences. This is because the method would introduce similar criteria and structure to assess compliance risks. According to the compliance manager, having such a framework “takes away the individual factor of risk where you have to depend on the individual”.

Second, by focusing on assessing the consequences of specific operational or technical risks, such an approach lacks proactivity in identifying all possible scenarios of noncompliance leading to similar consequences. This has its own downsides. On the one hand, it can lead to a repetitive task of assessing the consequences of different scenarios with the same consequences separately. This overlooks the fact that several scenarios combined could aggravate the contractual or legal consequences in point. The adoption of the integrated method, which primarily focuses on compliance requirements, would enable to deal with all potential sources that could lead to a specific contractual or legal consequence at one place. This avoids not only unnecessary effort but also enables the consideration of potential aggravated consequence when two or more scenarios are combined. Furthermore, the fact-based approach provides limited support for conducting compliance risk assessment of potential scenarios such as the focus of the case study. This is because the fact-based approach focuses on something happening in a real-world. The integrated approach is considered to “complete the risk picture”. Overall, the data from the case study does not disprove the hypothesis.

The following questions are asked for evaluating sub-hypothesis 2.

- What are the potential benefits of the graphical modelling? Does it enable good communication during and after the risk assessment among compliance, legal and security experts? Does the modelling enable systemized recording and communication of compliance risks?

Given that the compliance risk assessment in our case study involves the legal, compliance and IT experts, the use of the CORAS tool has proved to be very useful in facilitating the communication among these experts. The IT risk manager commented that “it was very easy to understand and I understand where it is going.” Similarly, the compliance manager indicated that “it always helps to put it into diagrams like that. It was very easy way of seeing what the input was and how the outcome was structured.” According to her, the advantage of the graphical modeling is that one can see the visual representation straight away, which is “very important because it stimulates and focuses discussions so that everyone is aware of what is being discussed and how, to a much greater extent than a meeting”. The legal counsel shared similar views indicating that a challenge within the current framework is that “we don’t talk the same language when we discuss risks, even when using the same words”. The visualization in CORAS is viewed to mitigate such communication problems. Such communication is also considered valuable even with similar group of people dealing with the operational risks. In the current framework, the compliance manager indicated, operational risks are discussed in risk forums and there is a value in facilitating such communication in such forms. In addition, by decomposing compliance norms into different elements through the natural language pattern and structuring these elements in a template, the approach simplifies the transition from normative statements (obligations or prohibitions) to the graphical risk models.

One of the main concerns raised against the graphical modelling is that it might not capture complex legal issues and interpretations provided in a case law. Similar concerns have been raised regarding missing information in the transition from the rules to the diagrams, thereby leading to a risk itself. These are valid concerns and need to be acknowledged. For example, the focus on obligations and prohibitions might overlook risks emanating from rights bestowed on other actors. Such rights might impose an obligation on the actor, which in turn could be source of risks. Similar risks might arise from the difficulty in capturing all information that give rise to risk. This is because often laws are drafted at an abstract level and there might be issues that require legal expert judgment, which could not be communicated through the CORAS models. This means, in some cases, the modelling can overly simplify the complexity of the issue at hand and hide disagreements. However, the challenge lies in balancing the need to introduce structure in conducting compliance risk assessments and the complexity inherent with regulatory rules. On the one hand, people working day-to-day business need to understand the relevant compliance requirements and associated risks that affect their activities. Given the business support would be more familiar working with risks than complex regulatory statements, the need for structuring and adapting to a system where they understand and deal with in their day-to-day business is crucial. On the other hand, care should be made to not oversimplify

complex legal issues. To mitigate the latter concern, when there are important issues that are not captured within the integrated framework and modelling, additional information could be provided in another format. Such challenge highlights the need for a more expressive language that can capture more information. Overall, the data from the case study does not disprove the hypothesis.

The following questions are asked for evaluating sub-hypothesis 3.

- Does the approach yield a positive cost-benefit ratio? Can the structured method be implemented without significant structural change to the organization? Is it possible (feasible) to conduct the structured risk assessment within the currently allocated resources?

It is indicated that the case provider follows a risk assessment framework, which is conducted as a bottom-up and top-down approaches. The method discussed in this paper fits well within the top-down approach. Also, it is indicated that the case provider has all the expertise to conduct the relevant exercise including lawyers, risk and compliance experts with experience in risk management. Thus, the integrated method would not require structural change and new expertise. However, the compliance risks need to be linked with the operational and technical risks in a manner that gives a good view to the management. To some extent, it is recognized that the results of the CORAS diagrams could be feed into the Archer tool – a tool used to document and communicate risks.

Time is an important issue in using the structured approach. “Time is money” commented one of the participants. It is true that the use of the structured approach would involve extra effort and time than using informal approaches. Particularly, the structuring of the requirements in the template and their modelling in CORAS entails some effort and money. Similarly, a consultation was made with the relevant Supervisory authority. However, time and cost issue should be looked in relation to the fact that the approach facilitates reusability. The legal counsel underlined the importance of such reusability in the face of organizational or regulatory changes. The creation of the generic risk models was considered to increase reusability. Given such risks are generic and based on the requirements means that there is no need to start from scratch every time there are changes in an organization or system. These generic risks can still be relevant so far as the requirements remain valid. Similarly, when only some parts of the law are changed, there is no need to redo the whole risk assessment so far as other things within the organization or the system remain unchanged. For example, the same generic risks identified in adopting the cloud services can be reused when introducing new ICT systems. The legal counsel commented that “reusability of the results is the most important benefit” of the method.

Furthermore, in the case study, it was possible for the risk analyst to come up with pre-identified generic threats that are used as a starting point for further analysis during the main sessions thereby reducing the time and effort. This is particularly important where the risk assessment involves participants with time constraints. Moreover, as part of the routine compliance assessment, requirements are structured in template very similar to the one used in the integrated method. This means that the current compliance framework generates information that can be reused when the integrated approach is employed. According to the compliance manager, given that there is already a structure, expertise, reusable information and a tool to document results, there is no significant additional cost in using the method. This implies that if an organization has separate compliance assessment and risk assessment frameworks in place, the cost-benefit assessment could be considered to be positive. Related with this, it is indicated that the integrated method is aimed at helping to conduct compliance risk assessments in certain contexts (e.g. when new legislation is adopted, moving to the cloud or when there is organizational change). This means that the cost implications are considered to be comparable to the benefits at stake in those contexts. In the words of the compliance manager, compared to the abovementioned benefits the cost and effort “is worthwhile”. Furthermore, the time and effort required in using the method would reduce as a result of experience. Given that the method is applied for the first time, it is likely that it would involve more time and effort than its subsequent uses. Thus, one can envisage a long-term cost-benefit resulting from the reusability and experience in using the method.

6 Summary

In this deliverable we have given an overview of the RASEN methodology and its instantiations to support risk-based compliance assessment, test-based security risk assessment and risk based security testing. Given this background, we have moreover demonstrated the wider relevance of RASEN by showing how it relates to and how it supports existing and established approaches to security assessment and secure system development. Furthermore, we have shown its applicability to security and compliance assessment beyond traditional ICT and information security by addressing the highly relevant domains of cybersecurity and cloud services.

The deliverable documents the third and final year results of WP5 regarding task T5.1 (Methodology for compositional and continuous risk assessment and security testing of large scale networked systems) and T5.2 (Methodology for legal risk assessment and security testing of large scale networked systems).

References

[1] Australian Standard AS 3806-2006 Compliance programs.

[2] Basel Committee on Banking Supervision. Compliance and the compliance function in banks. Bank for International Settlements (2005).

[3] Breaux TD, Antón AI (2005) Mining rule semantics to understand legislative compliance. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (WPES). ACM, New York, NY, USA, pp.51-54. DOI=10.1145/1102199.1102210

[4] Chatterjee A., and Milam D. Gaining Competitive Advantage from Compliance and Risk Management. In: Pantaleo, Pal D., and Nirmal (eds). From Strategy to Execution. Springer Berlin Heidelberg 2008, ISBN 978-3-540-71879-6.

[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Unleashing the Potential of Cloud Computing in Europe' COM (2012) 529 final (Commission Communication (2012) 529)

[6] COSO (2004) 'Enterprise Risk Management: An Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission

[7] Christian W Probst et al, 'Privacy Penetration Testing: How to Establish Trust in Your Cloud Provider' In S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* Springer, (Science and Business Media B.V.) 2012, 252.

[8] Darimont R, Lemoine M (2006) Goal-oriented analysis of regulations, REMO 2V06: Int. Workshop on Regulations Modelling and their Verification & Validation, Luxemburg. http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-241/paper9.pdf . Accessed 21 March 2015

[9] Deng M, Kim W, Riccardo S, Bart P, Woute J (2011) A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering 16(1): 3-32. doi: 10.1007/s00766-010-0115-7

[10] ENISA (2009) Cloud Computing: Benefits, risks and recommendations for information security. Catteddu D, Hogben G (ed) European Network and Information Security Agency

[11] Esayas, S and Mahler T, Modeling Compliance Risk: A Structured Approach Artificial Intelligence and Law (forthcoming)

[12] Esayas S, Mahler T, Seehusen F, Bjørnstad F, Brubakk V (2015) An Integrated Method for Compliance and Risk Assessment: Experiences from a Case Study. Paper to be presented at the IEEE Conference on Communications and Network Security, 28-30 September, 2015, Florence, Italy.

[13] Ghanavati S, A. Daniel, L. Peyton, "Comparative Analysis between Document-based and Model-based Compliance Management Approaches. Requirements Engineering and Law, 2008, pp.35-39. doi: 10.1109/RELAW.2008.2

[14] Ghirana, A., and Bresfelean, V.: Compliance Requirements for Dealing with Risks and Governance. Procedia Economics and Finance 3, pp. 752 – 756 (2012)

[15] Giblin, C., Liu, A.Y., Müller, S., Pfitzmann, B., and Zhou, X.: Regulations Expressed As Logical Models (REALM). In: Moens, M.-F., and Spyns, P. (Eds.), Legal Knowledge and Information Systems, pp. 37–48. IOS Press (2005)

[16] ETSI: TTCN-3

[17] Hohfeld WN (1913) Fundamental legal conceptions as applied in judicial reasoning. Yale Law Journal 23(1): 710-770

[18] IEEE: IEEE Standard for Software and System Test Documentation (IEEE 829-2008), ISBN 978-0-7381-5747-4, 2008.

[19] IEEE: IEEE Standard Glossary of Software Engineering Terminology (IEEE 610.12-1990), ISBN 1-55937-067-7, 1990.

[20] IEEE: IEEE 29119 Software and system engineering - Software Testing Part 1: Concepts and definitions, 2012.

[21] Information Commissioner's Office.:Privacy by Design. (ICO, November 2008), 2008.

[22] International Standards Organization. ISO 27000:2009(E), Information technology - Security techniques - Information security management systems - Overview and vocabulary, 2009.

[23] International Standards Organization. ISO 29119 Software and system engineering - Software Testing-Part 2 : Test process (draft), 2012

[24] International Standards Organization. ISO 31000:2009(E), Risk management – Principles and guidelines, 2009.

[25] ISTQB: ISTQB Glossary of testing terms version 2.2.http://www.istqb.org/downloads/finish/20/101.html, as of date 19.03.2013.

[26] Jorshari FZ, Mouratidis H, Islam S (2012) Extracting Security Requirements from Relevant Laws and Regulations. Research Challenges in Information Science (RCIS), Sixth International Conference pp.1-9. doi: 10.1109/RCIS.2012.6240443

[27] Kiyavitskaya N, Zeni N, Cordy JR, Breaux TD, Mich L, Antón AI, Mylopoulos (2007) Extracting Rights and Obligations from Regulations: Toward a Tool-Supported Process. ASE 2007, 22nd IEEE/ACM. In Conference on Automated Software Engineering, pp.429-432

[28] Mahler, T.: Tool-supported Legal Risk Management: A Roadmap. European Journal of Legal Studies 2(3), (2010). The Future of... Law & Technology in the Information Society.

[29] Mahler, T.: Legal Risk Management: Developing and Evaluating Elements of a Method for proactive legal analyses, with a particular focus on contracts. PhD thesis, University of Oslo, 2010

[30] Microsoft: The Microsoft Security Software Development Lifecycle, http://www.microsoft.com/en-us/sdl/default.aspx (last visited 09/2015)

[31] OCEG: GRC Capability Model. "Red Book" 2.0. http://www.oceg.org (2009)

[32] OMG: UML testing profile version 1.1 (formal/2012-04-01). http://www.omg.org/spec/UTP/1.1, as of date 19.03.2013

[33] Vondrák, I.: Business Process Modeling. In: M. Duží et al. (eds.) Information Modeling and Knowledge Bases XVIII, pp. 223-235. IOS Press (2007).

[34] Werf J.M., Verbeek, E., and Aalst, W.M.P.: Context-Aware Compliance Checking. In: Barros, A., Gal, A. and Kindler, E. (eds.): BPM 2012, LNCS 7481, pp. 98–113, 2012. Springer-Verlag Berlin Heidelberg (2012)

[35] Zoellick, B., and Frank, T., Governance, Risk Management, and Compliance: An Operational Approach. A Compliance Consortium Whitepaper, Public draft version 1 (2005).

[36] F. John Reh. www.about.com. http://management.about.com/cs/generalmanagement/g/objective.htm, last date accessed 28.08.2013.

[37] Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen: Model-Driven Risk Analysis, The CORAS Approach, Springer Verlag Berlin Heidelberg 2011, ISBN: 978-3-642-12322-1

[38] Terblanché J. R.: Legal risk and compliance for banks operating in a common law legal system. The Journal of Operational Risk 7(2), 2012.

[39] Testing Standards Working Party. BS 7925-1 Vocabulary of terms in software testing. 1998.

[40] Vicente P., and Silva, M.M.D.: A Business Viewpoint for Integrated IT Governance, Risk and Compliance. (IEEE World Congress on Services), ISBN: 978-07695-4461-8/11, 2011.

[41] RASEN Deliverable 4.3.1

[42] RASEN Deliverable 5.3.2

[43] G. Brændeland, A. Refsdal, K. Stølen: Modular analysis and modelling of risk scenarios with dependencies. Journal of Systems and Software 83(10), 1995-2013 (2010)

[44] J. M. Wing. A specifier's introduction to formal methods. IEEE Computer 23(9), 8,10-22,24 (1990)

[45] M. Broy and K. Stølen: Specification and Development of Interactive Systems: Focus on Streams, Interfaces and Refinement. Springer (2001)

[46] Zimmermann, F.; Eschbach, R.; Kloos, J. & Bauer, T.: Risk-based Statistical Testing: A Refinement-based Approach to the Reliability Analysis of Safety-Critical Systems EWDC 2009: Proceedings of 12th European Workshop on Dependable Computing, HAL - CCSD, 2009.

[47] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2011)

[48] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27032 – Information technology – Security techniques – Guidelines for cybersecurity (2005)

[49] National Institute of Standards and Technology: Guide for conducting risk assessments, special publ. 800-30 (2012)

[50] A. Refsdal, B. Solhaug, K. Stølen: Cyber-Risk Management. Springer (2015)

[51] A. S. Tanenbaum: Computer networks, 4 edn. Prentice Hall (2003)

[52] Vraalsen F, Lund MS, Mahler T, Parent X, Stølen K (2005) Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language: Experiences and the Way Forward. In: Herrmann P et al (ed) iTrust, LNCS, vol. 3477, pp.45–60. Springer, Heidelberg

[53] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/sme-guide-tool

[54] Rossebø, J., Cadzow S., and Sijben, P.: eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope. In AReS ’07: Proceedings of the The Second International Conference on Availability, Reliability and Security, pages 925–933. IEEE Computer Society, 2007.