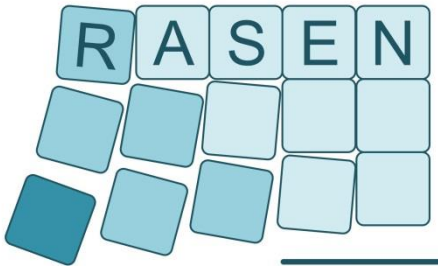

Compositional Risk Assessment and Security Testing of Networked Systems

Deliverable D5.3.1

Methodologies for Legal, Compositional, and Continuous Risk Assessment and Security Testing v.1

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:	D5.3.1
Nature of deliverable:	Report
Dissemination level:	PU
Internal version number:	1.0
Contractual delivery date:	2013-09-30
Actual delivery date:	2013-09-30
Responsible partner:	SINTEF

Contributors

Editor(s)	Fredrik Seehusen (SINTEF)
Contributor(s)	Jürgen Großmann (Fraunhofer), Tobias Mahler (UiO), Fredrik Seehusen (SINTEF), Bjørnar Solhaug (SINTEF), Ketil Stølen (SINTEF)
Quality assuror(s)	Arthur Molnar (Info World), Fabien Peureux (Smartesting)

Version history

Version	Date	Description
0.1	13-06-10	Table of contents with partner roles
0.2	13-07-05	Added overview in methodology section
0.3	13-08-06	Input from UIO and FOKUS
0.4	13-08-29	Input from SMA
0.5	13-08-28	Input from SINTEF
0.6	13-09-04	Additions from FOKUS
0.6	13-09-08	Input from UiO
0.7	13-09-09	Added introduction and summary. Editorial updates made.
1.0	26-09-09	Finalized document, comments from internal reviewers implemented

Abstract

This deliverable documents the conceptual models and initial version of the methodologies related to tasks T5.1 and T5.2.

Keywords

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

Executive Summary

This document constitutes the first version of the RASEN methodologies related to task T5.1 and T5.2 in work package 5.

First we provide conceptual models for the three main domains that are addressed by the RASEN project: (security) testing, (security) risk assessment, and legal risk assessment. The conceptual models define the most essential terms and their relationships within the three domains. Second, we define three generic baseline methodologies that address compositional test-based risk assessment (i.e. the use of testing for improving the risk assessment), risk-based testing (the use of risk assessment to improve the testing), and legal risk assessment. The generic methodologies serve as a starting point for defining the initial RASEN methodologies which should be seen as instances or refinements of the generic methodologies. Finally, we describe the initial RASEN methodologies.

Table of contents

1 Introduction

The overall objectives of WP5 are to (1) develop a methodology that integrates the techniques developed in WP3 and WP4, (2) develop a methodology which takes into account risk assessment in legal contexts, and (3) develop a toolbox that integrates the tools developed in WP3 and WP4.

This document addresses objectives (1) and (2), and it constitutes the first version of the RASEN methodologies. The deliverables addresses methodologies that combine risk assessment with testing as well as composition (Section 3.3). Continuous assessment will be considered in will considered in the next versions of this deliverable.

First, in Section 2 we define a conceptual model for the RASEN methodologies. The conceptual model defines central terms and their relationships within the domains that are addressed by RASEN: testing, security testing, risk assessment, security risk assessment, and legal risk assessment. The conceptual model ensures that the central terms used in the process descriptions of the methodologies are clearly defined and understood. In addition to this, the conceptual model has served as a starting point for defining the data model which is the basis for the RASEN tool integration, documented in the companion deliverable D5.4.1.

In Section 3, we define generic methodologies that serve as a baseline/starting point for the definition of the RASEN methodologies. The intention is that the RASEN methodologies will be instances or refinements of these generic methodologies. We describe four generic methodologies. The first two address the combination of risk assessment and testing: one of these incorporates the test process into the risk assessment process, whereas the other incorporates the risk assessment process into the test process. The third methodology addresses the use of composition within a test-based risk assessment process, and the forth addresses legal risk assessment.

In Section 4, we define the initial RASEN methodologies. All the methodologies are described in the same way by using a template to document each step/activity in the processes. The first methodology addresses risk-based testing with particular emphasis on the use of so-called patterns as means of deriving tests from the risk model. The second methodology addresses test-based risk assessment with particular emphasis on the use of the risk model for prioritization and selection of test procedures. The third and final methodology, addresses legal risk assessment.

In Section 5, we provide a summary of this document.

2 A Conceptual Model for the RASEN Methodologies

2.1 Testing

Testing and especially software testing is an analytical approach to evaluate a system or a software system for compliance with a set of requirements that have been defined for the use and the quality of a system. The findings are used to detect and correct software errors. Testing is normally integrated in the software development process and thus an essential part of software development. In general we can distinguish dynamic and static test approaches. While dynamic testing evaluates the system when it is under execution, static testing addresses the quality of the program code, models, and other artifacts from the development process. Dynamic testing is one of the best known and most used quality assurance measures with many different techniques that are of great importance in practice. Most of the techniques are relatively well known and are already established. Nevertheless, there have been many advances for test automation and model-based testing in industrial practice through the introduction of techniques which aim in particular to systematize and automate the testing.

Standards like IEEE 829 [7], ISO/IEC/IEEE 29119 [9], the ISTQB Glossary of testing terms [14], and the UML Testing Profile (UTP) [18] define the basic activities and related artifacts of a testing process. The major activities can be characterized as follows:

- Test planning (results: a test plan containing test conditions, test techniques, test coverage items and test completion criteria)
- Test design& implementation (results: test cases and test procedures)
- Test execution (results: test logs and test results)
- Test evaluation & incident reporting (result: test incidents reports and test incidents)

Since the RASEN project focuses on the relationship between risk assessment and testing, the following model especially reflects the terms and concepts that are in our view relevant to describe the interfaces between testing and risk assessment. In this sense the model concentrates on activities like test planning and test specification as well as the management, evaluation and interpretation of the test results. The following model is mainly based on terms and concepts taken from ISO 29119.

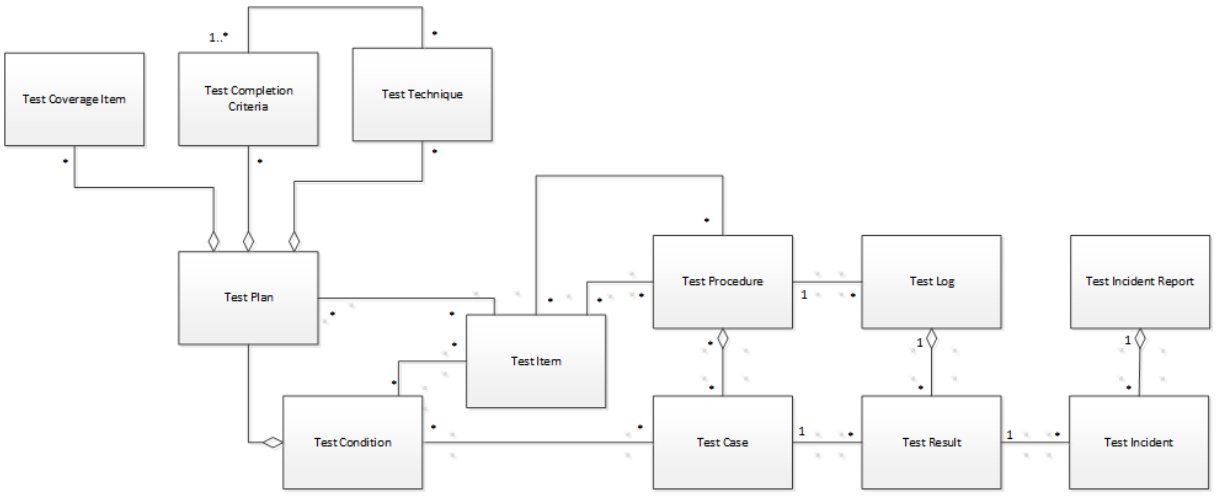

Figure 1 – Basic testing concepts

Test item – is a work product (e.g. system, software item, requirements document, design specification, user guide) that is an object of testing [9].

Test condition – is a testable aspect of the test item (i.e. a component or system), such as a function, transaction, feature, quality attribute, or structural element identified as a basis for testing [9].

Test case – is a set of preconditions, inputs (including actions, where applicable), and expected results, developed to determine whether or not the covered part of the *test item* has been implemented correctly [9].

Test procedure – is **a** sequence of *test cases* in execution order, and any associated actions that may be required to set up the initial preconditions and any wrap up activities post execution [9].

Test plan – is a detailed description of test objectives to be achieved and the means and schedule for achieving them, organized to coordinate testing activities for some test item or set of test items [9]

Test coverage item – is an attribute or combination of attributes to be exercised by a *test case* that is derived from one or more *test conditions* by using a test design technique [9].

Test completion criteria – are a set of generic and specific conditions, agreed upon with the stakeholders, for permitting a testing process or a testing sub process to be completed.

Test (design) technique – is a compilation of activities, concepts, processes, and patterns used to identify *test conditions* for a *test item*, derive corresponding test coverage items, and subsequently derive or select test cases [9].

Test log – is a recording which tests cases were run, who ran them, in what order, and whether each test passed or failed (IEEE 829 [7], ISO/IEC/IEEE 29119 [9]).

Test result – is an indication of whether or not a specific test case has passed or failed, i.e. if the actual result corresponds to the expected result or if deviations were observed [9]. Relevant testing standards [18] refer to test results with the values *none*, *pass*, *inconclusive*, *fail* and *error*.

Test incident – is an event occurring during testing that requires investigation (ISTQB [18]).

Test incident report – is a detailed description for any test that failed. It contains the actual versus expected result and other information intended to throw light on why a test has failed. The report consists of all details of the incident such as actual and expected results, when it failed, and any supporting evidence that will help in its resolution. The report will also include, if possible, an assessment of the impact of an incident upon testing (IEEE 829 [7], ISO/IEC/IEEE 29119 [9]).

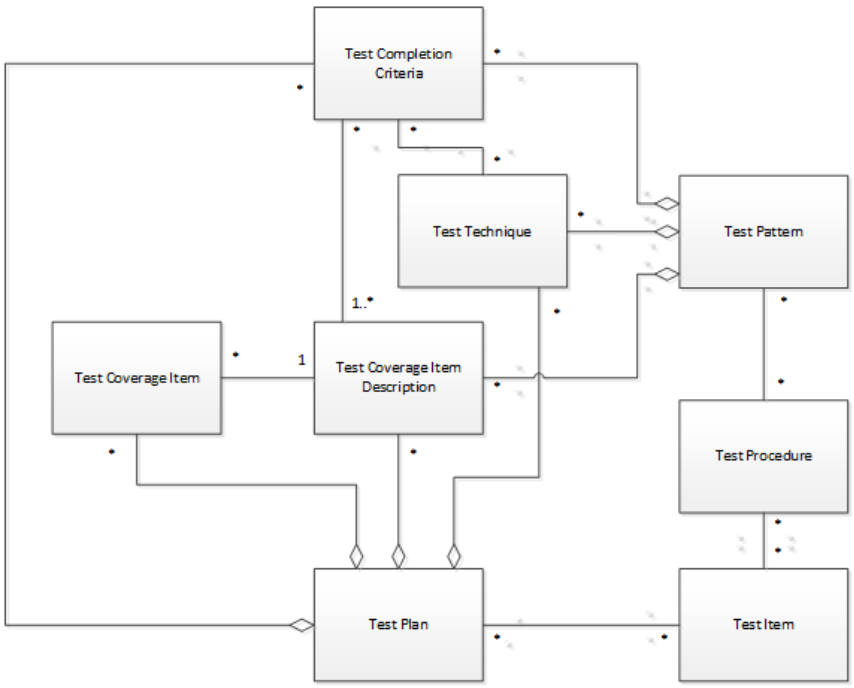

Figure 2 – Test pattern

Test pattern – is a collection of best practices/solutions for a known testing problem. It assembles reusable parts of a test plan, e.g. the test design techniques and corresponding test completion criteria, a test coverage item description, applicable test and coverage metrics, estimation on the necessary testing efforts and estimation of test effectiveness with respect to the given problem. Additionally it may contain also test data and specification and assumptions on the test environment as well as testing tool requirements.

2.2 Security Testing

Security testing is used to experimentally check software implementations with respect to their security properties and their resistance to attacks. For security testing we can distinguish functional security testing and security vulnerability testing. Functional security testing checks if the software security functions are implemented correctly and consistent with the security functional requirements. It is used to check the functionality, efficiency and availability of the specified security features of a test item. Security vulnerability testing directly addresses the identification and discovery of yet undiscovered system vulnerabilities. This kind of security testing targets the identification of design and implementation faults that lead to vulnerabilities that may harm the availability, confidentiality and integrity of the test item.

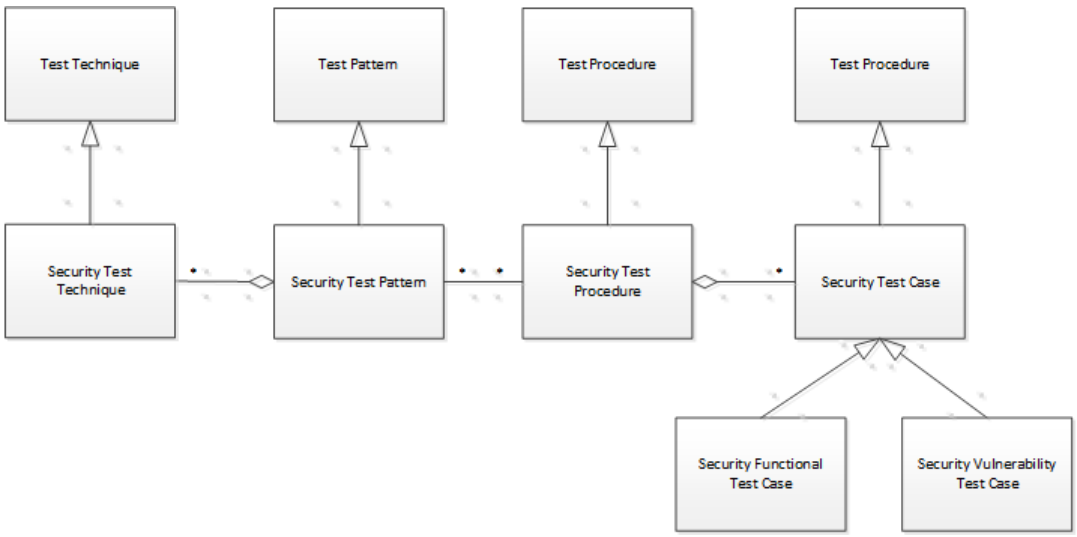

Figure 3 – Security testing

Security test case – is a set of preconditions, inputs (including actions, where applicable), and expected results developed to determine whether the security features of a *test item* have been implemented correctly or to determine whether or not the covered part of the *test item* has vulnerabilities that may harm the availability, confidentiality and integrity of the test item.

Security functional test case – is a security test case that checks if the software security functions are implemented correctly and consistent with the security functional requirements. It is used to check the functionality, efficiency and availability of the specified security features of a test item.

Security vulnerability test case – is a security test case that directly addresses the identification and discovery of yet undiscovered system vulnerabilities. This kind of security testing targets the identification of design and implementation faults that lead to vulnerabilities that may harm the availability, confidentiality and integrity of the test item.

Security test procedure – is a sequence of *security test cases* in execution order together with any associated actions that may be required to set up the initial preconditions and any wrap up activities post execution.

Security test (design) technique – is a collection of activities, concepts, processes, and patterns used to identify test conditions for a test item, derive corresponding test coverage items, and subsequently derive or select test cases to test security properties and to test for vulnerabilities.

Security test pattern – is a collection of best practices/solutions for a known security testing problem. It assembles reusable parts of a test plan e.g. the security test design techniques and corresponding test completion criteria, a test coverage item description, applicable test and coverage metrics, estimation on the necessary testing efforts and estimation of test effectiveness with respect to the given problem. Additionally it may contain also test data and specification and assumptions on the test environment as well as testing tool requirements.

2.3 Risk Assessment

The conceptual model and notions defined here are based on the ISO 31000 standard [13].Figure 4 shows the conceptual model for risk assessment.

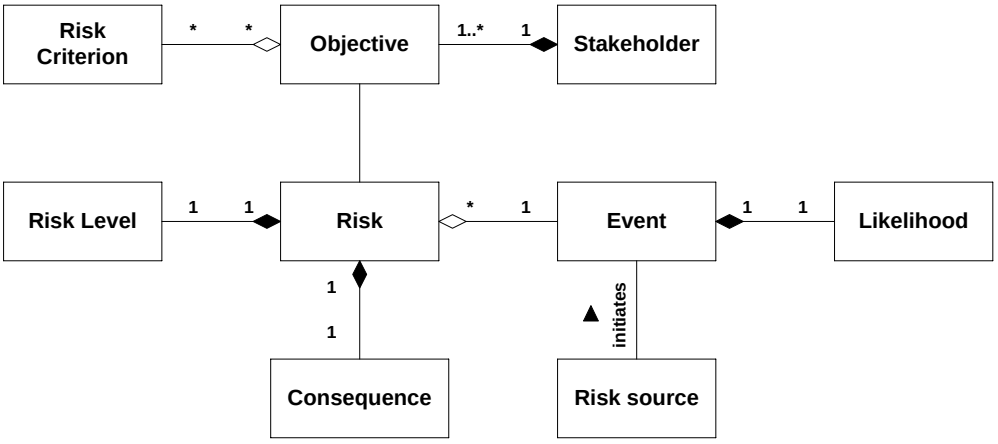

Figure 4 – Conceptual model for risk assessment

The terms of the model are defined in the following.

Risk – the combination of the consequences of an event with respect to an objective and the associated likelihood of occurrence (adapted from [13]).

Objective – something the stakeholder is aiming towards or a strategic position it is working to attain (adapted from [26]).

Risk Source – an element which alone or in combination has the intrinsic potential to give rise to risk [13].

Stakeholder – a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity [13].

Event – the occurrence or change of a particular set of circumstances [13].

Likelihood – the chance of something happening [13].

Consequence – the outcome of an event affecting objectives [13].

Risk Criterion – the term of reference against which the significance of a risk is evaluated [13].

Risk Level – the magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood [13].

2.4 Security Risk Assessment

Lund et al. [14] classify risk analysis approaches into two main categories:

- Offensive approaches: Risk analysis concerned with balancing potential gain against risk of investment loss. This kind of risk analysis is more relevant within finance and political strategy making.
- Defensive approaches: Risk analysis concerned with protecting what is already there.

In the context of security, the defensive approach is the one that is relevant.

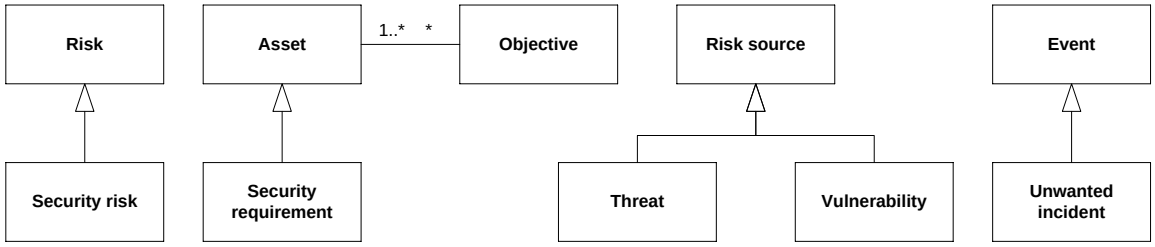

Figure 5 – Conceptual model for security risk assessment

The main terms related to security risk assessment and their relationship to previously defined terms in the risk assessment domain are illustrated in Figure 5. In the following we define the terms (for the definitions of Risk, Objective, Risk source and Event see Section 2.3).

Security Risk Assessment – The process of risk asset specialized towards security.

Asset – Anything that has value to the stakeholders (adopted from [11]).

Security Requirement – A specification of the required security for the system (adopted from [29]).

Security Risk – A risk caused by a threat exploiting a vulnerability and thereby violating a security requirement.

Unwanted Incident – An event representing a security risk.

Threat – Potential cause of an unwanted incident [11].

Vulnerability – A weakness of an asset or control that can be exploited by a threat [11].

2.5 Legal Risk Assessment

2.5.1 Legal Risk Management

Legal risk management is a subset of the wider concept of risk management. Mahler [16] defines legal risk management as a set of coordinated activities to direct and control an organization with regard to the:

1. management of legal risk and
2. legal management of risk

Mahler's definition of legal risk management is in line with the ISO 31000 Risk Management – Principles and Guidelines [13], but makes a distinction between two aspects of legal risk management. When risk management is applied with a focus on risks that have legal issue as their source, it constitutes the management of *legal risk* [16]. The legal management of risk, on the other hand, focuses on the management of non-legal risks by legal means [16]. However, legal issues in the context of risk become more vivid in the management of *legal risk* [15].

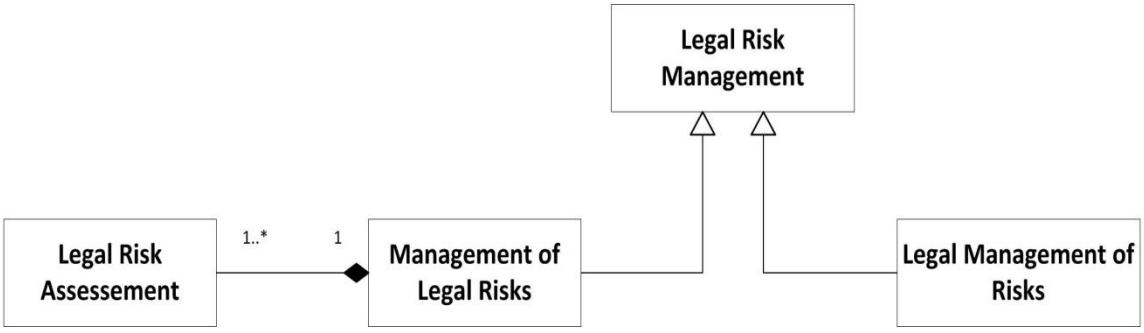

Figure 6 – Legal risk management

As shown in the figure above, the management of legal risk involves one or more legal risk assessments. The conceptual model for legal and compliance risk analysis is shown inFigure 7.The concepts described here are primarily based on [16], which in turn is built on the ISO 31000 standard [13]**.**

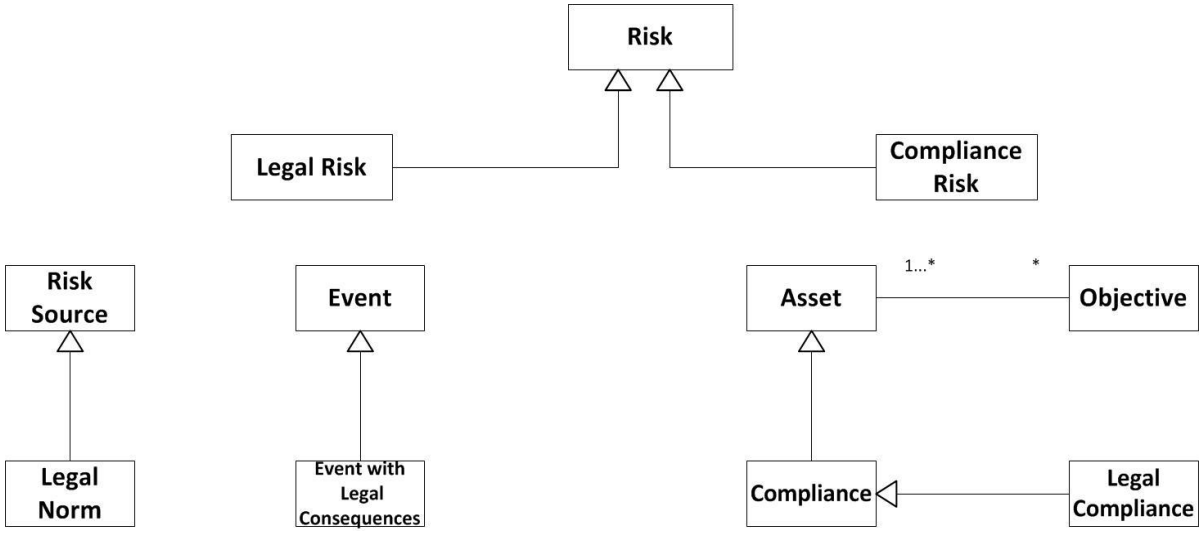

Figure 7 – Conceptual model for legal and compliance risk analysis

Legal risk assessment – is the process of risk assessment focusing on legal risk.

Compliance risk assessment – is the process of risk assessment focusing on compliance risk.

Legal risk – is a risk that has a legal issue as its source. Legal issue on the other hand is a set of facts that are assessed under a set of legal norms.

Legal norm – is a norm that is based on a legal source.

Compliance – is defined in [1] as adhering to the requirements of laws, industry and organizational standards and codes, principles of good governance and accepted community and ethical standards. According to [1], an effective organization-wide compliance should enable an organization to demonstrate its adherence with relevant laws, including legislative requirements, industry codes, organizational standards as well as standards of governance, ethics and community expectations. Therefore, the ability to demonstrate compliance forms an essential component of an organization's compliance framework. In this regard, the Open Compliance & Ethics Group (OCEG) [17] underlines that compliance involves not only the act of adhering but also the ability to demonstrate adherence.

Legal compliance – is adhering to the requirements of the law.

Compliance risk – a risk resulting from failure to comply with laws, regulations, rules, related self-regulatory organization standards, and applicable codes of conduct [2].

Event with legal consequences – an event giving rise to legal consequences (such as potential penalties, contractual damages and regulatory action).

Despite some overlap between legal and compliance risk, it is also worth noting that there is an important distinction between the two concepts. As shown in Figure 8 below, compliance risk can be an aspect of legal risk when the source of the latter is failure to comply with legal norms including contractual undertakings. Nevertheless, legal risk also includes risks resulting from legal uncertainty which does not pertain to compliance risk. Examples of such legal risks include the exposure to new laws, adverse interpretation of and/or unenforceability of contractual provisions as well as changes in interpretations of existing law(s). On a similar note, when the source of compliance risk emanates from legal norm, it constitutes one aspect of legal risk. But not all compliance risks result from failure to comply with legal norms.

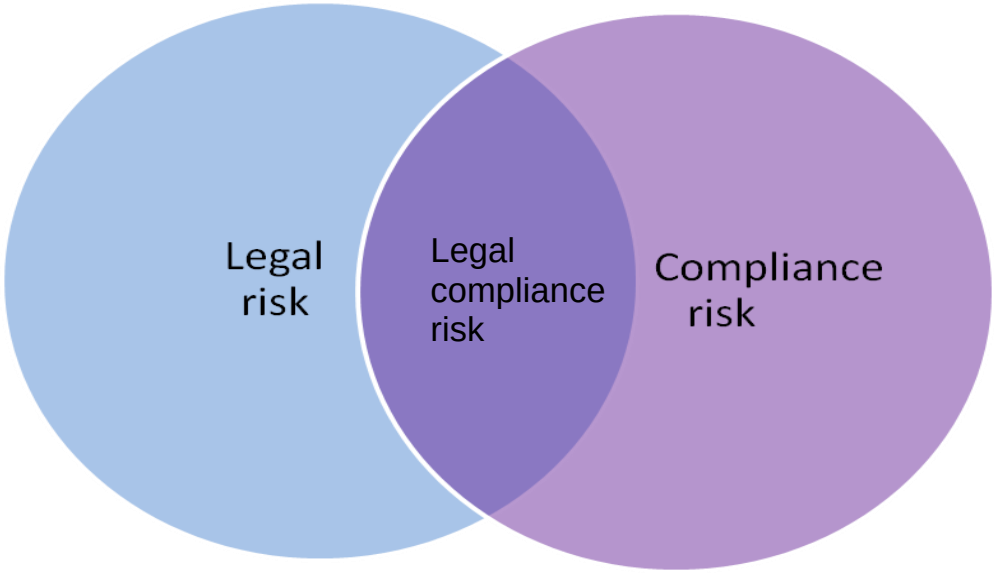

Figure 8 – Legal risk and compliance risk

The table below gives a description and an example for each of the three risks represented in the Venn diagram.

Type of risk	Description	Example
Legal risks which are not compliance risks	The risk that an unceratin legal issue gives rise to unwanted legal consequences	**Cause:** change in the interpretation of the existing legal requirements or introduction of new legal requirements **Consequence:** failure to get an authorization for processing medical data
Compliance risks which are not legal risks	The risk resulting from failure to comply with internal policies, industry and organizational standards and codes, principles of good governance and accepted community and ethical standards (non-legal sources)	**Cause**: failure to comply with the internal policies regarding time period for handling customer requests **Consequence:** loss of customers
Legal Compliance risk	The risk resulting from failure to adhere to the requirements of the law	**Cause:** failure to comply with the 'explicit consent' requirement to process medical data **Consequence:** monetary fine and discontinuation of further processing

Table 1 – Distinct attributes of legal risk, compliance risk and legal-compliance risk

2.5.2 Compliance Management

The globalization and recent corporate scandals have led to the introduction of myriad of new regulations directed towards businesses [5]. Not only the sheer number of laws and standards are drastically increasing but also are becoming more complex [5]. This has resulted in a growing interest, in research as well as business practice, over compliance management in recent years [4]. The definition of risk management within the ISO 31000 [13] is used as a basis for defining compliance management in the interest of consistency with other concepts in this section and the rest of the project. Accordingly, compliance management can be referred as a set of coordinated activities to direct and control an organization with regard to compliance (risk). In recent discussions, both the term risk management and compliance management are often referred as components of an integrated GRC (Governance, Risk and Compliance) approach. Although definitions might vary depending on the context, Racz et al [21] derived a comprehensive definition based on literature review and an online expert survey, which they consider as 'scientifically developed and validated' definition of integrated GRC. According to [21], integrated GRC is referred as: "… an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations, through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness." Zoellick and Frank [25] consider the three concepts as 'a package deal' where the effectiveness and sustainability of compliance relies on an ongoing board-level engagement in governance and risk management, and where compliance is the means to support governance and risk management. Of particular relevance in the context of this report is to elaborate the relationship between legal risk management and compliance management.

While one can hardly deny the existence of some link between legal risk management and compliance, the exact relationship warrants some clarification. The relationship between the two concepts is akin to the relationship between legal risk and compliance risk noted above. When legal risk management focuses on managing risks resulting from failure to comply with legal norms or contractual undertakings, legal risk management becomes an aspect of compliance management. However, legal risk management could also involve the management of risks resulting from, for instance, legal uncertainty which does not pertain to compliance. Similarly, when compliance management focuses on complying with legal norms (legal compliance), it constitutes an integral part of the legal risk management. But compliance management also includes compliance with non-legal norms. Yet to the extent that the risks resulting from failure to comply with non-legal norms can be managed by legal-means, they still remain an integral part of legal risk management. Because legal risk management is not just about the management of legal risks but also the management of non-legal risks through legal means.

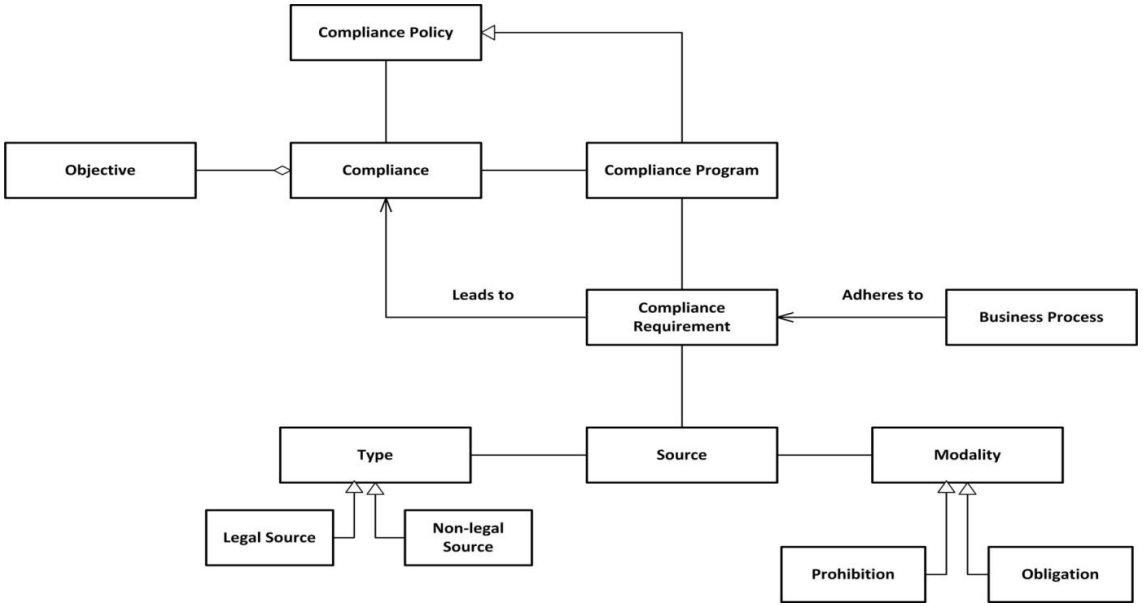

Figure 9 – Conceptual model for compliance management

Compliance policy – a set of principles and responsibilities with respect to achieving compliance [1].

Compliance program – a series of activities that when combined are intended to achieve compliance [1].

Compliance requirement – is a requirement that needs to be complied with. Such requirement can emanate from *legal or non-legal sources,* the *modality* of which can be *prohibition or obligation.*

Obligation – specific actions that the organization must undertake in order to comply with the corresponding compliance requirement.

Prohibition – specific actions that the organization must not undertake in order to comply with the corresponding compliance requirement.

Business process – a set of one or more linked procedures or activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships [23].

2.5.3 Audit Management

The activity of compliance checking is commonly referred to as auditing [24]. Essentially, auditing is the process of checking that the compliance requirements are being met and the control measures at critical points are adequate [1]. Checking compliance requires conducting different auditing tests which might include technical and/or non-technical testing. Figure 10 shows the conceptual model for Audit management.

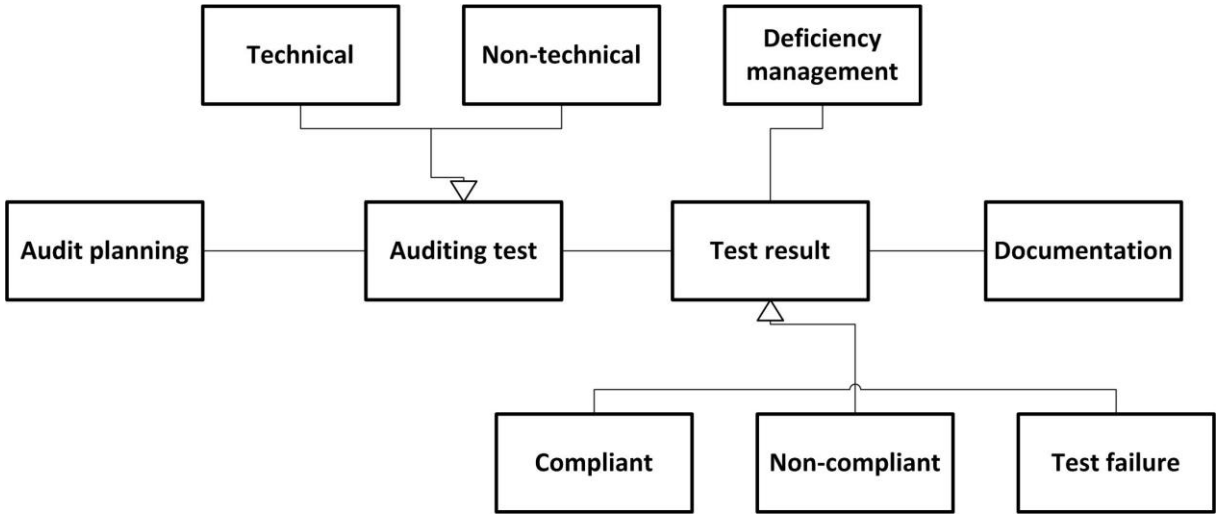

Figure 10 – Conceptual model for audit management

Audit planning – is the process of defining the scope, steps, time (start/end) of the audit and the persons responsible. In defining the scope of the auditing focus should be given to high risk areas as highlighted in the risk assessment part.

Auditing test – is a test run to check whether the business execution adheres to the defined compliance requirements and checking the suitability and effectiveness of the control measures put in place as a result of the risk and compliance management. Auditing test can involve both technical and non-technical testing.

Nontechnical testing – involves evaluating and testing the effectiveness in the implementation of plan policies, procedures and business processes. This could be done, for instance, by selecting high risk departments and reviewing their policies and procedures to determine if there is a gap between those policies and procedures and the compliance requirements through observation of business procedures, inquiry into and examination of different documentations and interactions. It also involves evaluating documented administrative procedures pertaining to the selection and execution of certain compliance measures. For instance, for purposes of information security, non-technical testing involves checking that physical computer system and related buildings and equipment for protection from fire and other natural environmental hazards, including intrusion.

Technical testing – evaluates the effectiveness and correct implementation of the technical measures in place that protect information, control individual access to information and that guard against unauthorized access to data transmitted over a communications network. A detailed description of such testing and related concepts is provided in Section 2.2.

Test result – the consequence/outcome of an auditing test. A test result is recorded as a test failure when the test is not completed. Whereas if the result of the test shows that the control system is effective and adequate, it can be recorded as compliant. A test result is considered as non-compliant if the test shows that certain controls are ineffective or inadequate.

Deficiency management – is a process that triggers actions for tests which are not complete or ineffective in order to restore the integrity of the internal control system.

Assessing risks and placing controls is a fundamental step towards ensuring compliance. But it is also important for organizations to make sure that their internal control system is ready for an audit (internal or external) at any time. In other words, legal risk and compliance management focuses not only on ensuring that there are adequate controls to address legal and compliance risks, but also that appropriate controls, conduct and behaviors are being checked ensuring that undesirable conduct is not occurring. This calls for complete and audit-acceptable documentation, through keeping accurate, up-to-date records of the organization's compliance activities, and monitoring of controls, conducted tests as well as the alleged compliance failures and the steps taken to resolve them. The documentation should be organized in a way that best suits the target group i.e., for external or

internal auditors or management. In this regard, it is important to underline that the approach/methodology employed by organizations in managing their legal and compliance risks has a vital role towards the achievement of such objectives. Employing a systematic way of identifying, assessing and documenting risks and control measures would enable organizations prepare their internal control system for external auditors, such as regulators, without a great deal of extra work. Besides documentation, the Australian Standard [1] notes that organizations should be able to demonstrate compliance through practice. This typically includes:

a. Adequate resourcing of the compliance program

b. Necessary investment in compliance training to reflect its importance

c. Linking compliance behavior to incentives and performance management

3 RASEN Generic Baseline Methodologies

In this section we describe four generic processes that serve as a baseline for the definition of the initial RASEN methodologies. The intention is that the initial RASEN methodologies should be seen as instances of the generic baseline methodologies.

First we describe a general process for test-based risk assessment in which the testing has been integrated in a risk assessment process, and then a process for risk-based test assessment in which the risk assessment has been integrated into a testing process. Third, we discuss the use of composition within a process for test-based risk assessment, and finally we describe a generic process for legal risk assessment.

3.1 Test-based Risk Assessment

In Figure 11, we have illustrated the main steps of the generic process for test-based risk assessment that is and will be used as a basis for defining the RASEN methodologies. The left hand side of the figure shows a standard risk assessment process whose activities are based on ISO 31000 Risk management standard [13]. As shown on the right hand side of the figure, there are two places where testing can in principle be used to enhance the risk assessment process. The first is between the steps "establish objective and context" and "risk identification". The idea here is that testing techniques (such as techniques for network or vulnerability discovery) can be used as input for the risk identification step. The second is between the steps "risk evaluation" and "risk validation and treatment", where the idea is that testing can be used as a means of validating the correctness of the risk model.

In the following, we describe each step of the process in more detail.

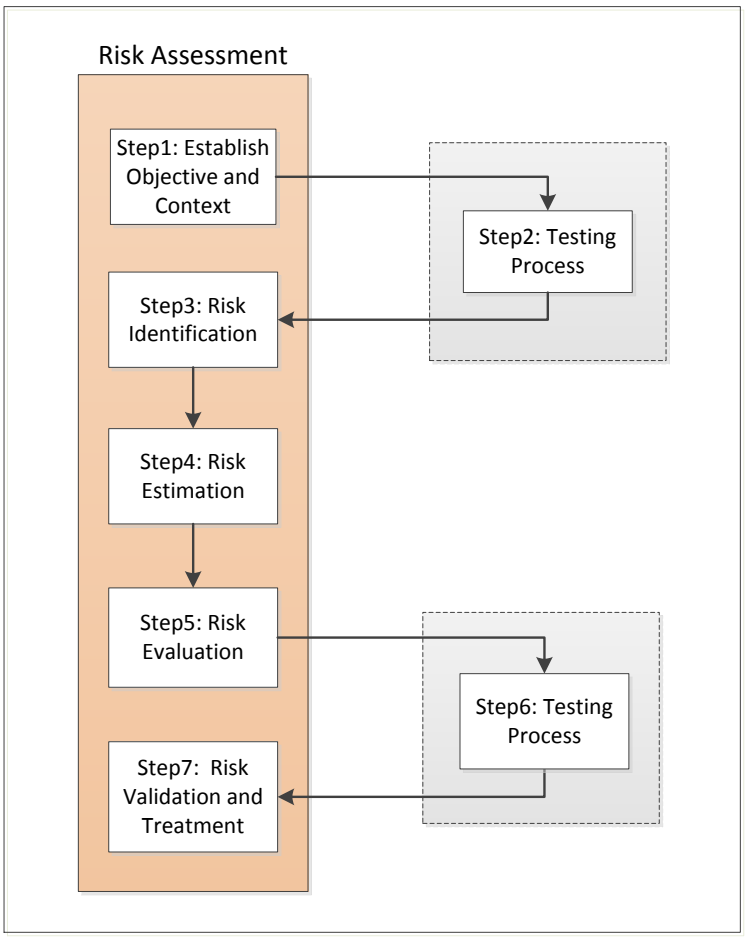

Figure 11 – Generic process for test-based risk assessment

Step 1: Establish Objective and Context

Establishing the context refers to the process of defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the remaining process (adapted from [13]).

Input: Objective, security requirement

Output: Assets that need to be defended, risk criteria, system model

Step 2: Testing Process

In this context, testing process refers to the process of using testing for identifying/discovering threat test scenarios or areas or vulnerabilities where the risk assessment should be focused. This may be performed by e.g. use of network discovering techniques or vulnerabilities scanners.

• **Input:** Assets that need to be defended, risk criteria, system model

• **Output:** Test log and test incident report

Step 3: Risk Identification

Risk identification is the process of finding, recognizing and describing risks. This involves identifying sources of risk, areas of impacts, events (including changes in circumstances), their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs [13].

• **Input**: Assets that need to be defended, system model, test log, test incident report

• **Output:** Incomplete risk model

Step 4: Risk Estimation

Risk estimation is the process of comprehending the nature of risk and determining the level of risk. This involves developing an understanding of the risk. Risk estimation provides the basis for risk evaluation and decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods (adapted from [13]).

• **Input:** Assets that need to be defended, risk criteria, system model, incomplete risk model

• **Output:** Risk model (with estimated likelihood and consequence values)

Step 5: Risk Evaluation

Risk evaluation is the process of comparing the results of risk estimation with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (adapted from [13]).

• **Input:** Assets that need to be defended, risk criteria, risk model

• **Output:** Risk prioritized with respect to risk criteria

Step 6: Testing Process

In this context, testing process refers to the process of using testing to validate the correctness of the risk model.

• **Input:** Assets that need to be defended, system model, risk model, risk prioritized with respect to risk criteria

• **Output:** Test log and test incident report

Step 7: Risk Validation and Treatment

Risk validation refers to the process of validating or updating the risk model based on the risk assessment results. Risk treatment is the process of modifying risk which can involve risk mitigation, risk elimination or risk prevention (adapted from [13]).

• **Input:** Assets that need to be defended, risk criteria, risk model, test log, test incident report

• **Output:** Treatment, updated risk model.

3.2 Risk-based Testing

In this section we describe a generic process for risk-based testing that will serve as a baseline for the RASEN methodologies. The main steps of the process are shown in Figure 12. The left hand side of the figure shows the steps of a testing process based on the upcoming international standard ISO/IEC 29119 Software Testing [9]. Furthermore, the figure indicates two areas where the testing process can be improved by risk assessment. The first is between the steps "test planning" and "test design & implementation", where risk assessment can be uses for test identification, and test selection/prioritization. The second is between "test environment set up & maintenance" and "test execution" where risk assessment can be used to prioritize *executable test cases*.

In the following, we describe the steps of the process in more detail.

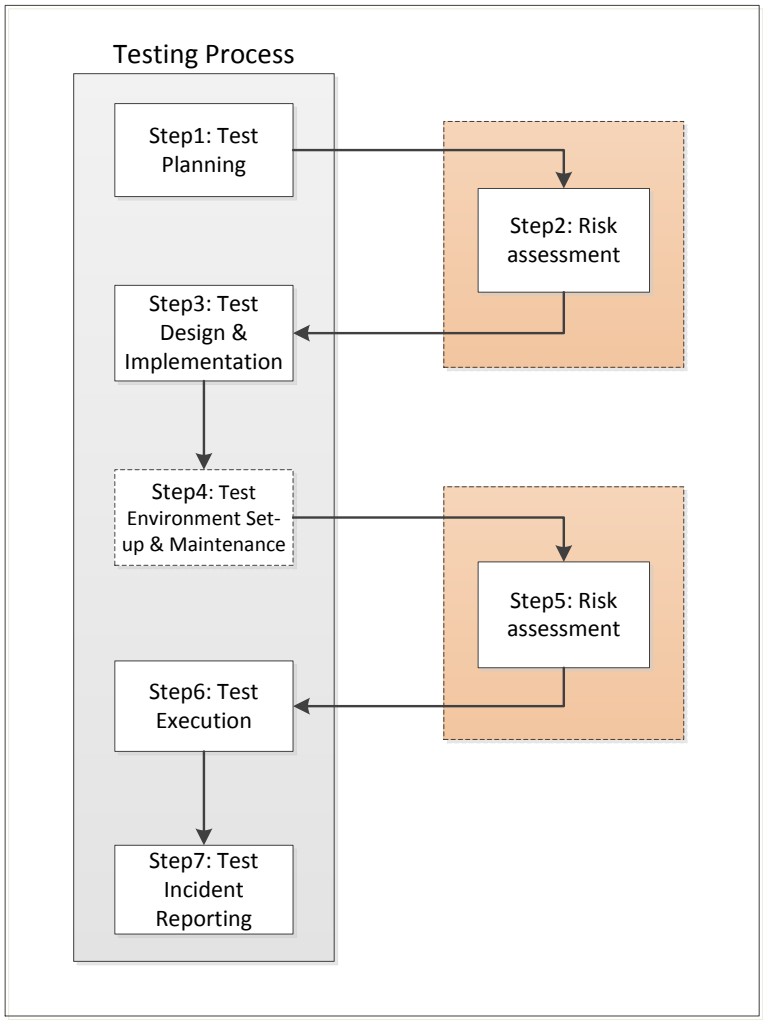

Figure 12 – Generic process for risk-based testing

.

Step 1: Test Planning

The test planning is the activity of developing the test plan. Depending on where in the project this process is implemented this may be a project test plan or a test plan for a specific phase, such as a system test plan, or a test plan for a specific type of testing, such as a performance test plan (adapted from [12]).

• **Input:** Test policy, system model

• **Output:** Test plan, security test requirement

Step 2: Risk Assessment

In this context**,** risk assessment refers to the process of using risk assessment to identify and prioritize test procedures that will be used as a starting point for test design.

• **Input:** System model, security test requirement

• **Output:** Risk model, risk criteria, prioritized security risks with respect to risk criteria

Step 3: Test Design and Implementation

The test design and implementation is the process of deriving the test cases and test procedures (adapted from [12]).

• **Input**: Risk model, risk criteria, prioritized security risks with respect to risk criteria, test plan, system model, security test requirement

• **Output:** Test case, test procedure

Step 4: Test Environment Set-up and Maintenance

The test environment set-up and maintenance process is the process of establishing and maintaining the environment in which tests are executed (adapted from [12]).

• **Input:** Test plan, system model, test, test procedure

• **Output:** Test environment model

Step 5: Risk Assessment

In this context, risk assessment refers to the process of using risk assessment to prioritize the test cases which should be executed.

• **Input:** System model, test model, security test requirement

• **Output:** Risk model, risk criteria, prioritized security risks with respect to risk criteria

Step 6: Test Execution

The test execution is the process of running the test procedure resulting from the test design and implementation process on the test environment established by the test environment set-up and maintenance process. The test execution process may need to be performed a number of times as all the available test procedures may not be executed in a single iteration (adapted from [12]).

• **Input**: Risk model, risk criteria, prioritized security risks with respect to risk criteria, test plan, test, test procedure, test environment model

• **Output:** Test result, test log

Step 7: Test Incident Reporting

The test incident reporting is the process of managing the test incidents. This process will be entered as a result of the identification of test failures, instances where something unusual or unexpected occurred during test execution, or when a retest passes (adapted from [12]).

• **Input:** Test result, test log

• **Output:** Test log, test incident report

3.3 Compositional Security Risk assessment and Testing

By compositional assessment we mean a process for assessing separate parts of a system or several systems independently, with means for combining separate assessment results into an overall result for the whole system [32]. The dual of composition is decomposition, which is a well-known feature from system specification and design [33]. Decomposition is the process of partitioning a system specification into separate modules that can be developed and analyzed independently, thus breaking the development problem into more manageable pieces. Each module may moreover be developed at different sites, by independent teams, or within different companies [34].

In the literature, composition is mainly addressed at the level of techniques, mostly with respect to languages, and we are not aware of any methodology for risk assessment that explicitly addressed the

use of composition. However, such a methodology should address *how* and *why* composition should be used. In the following, we identify areas in the process for test-based risk assessment where composition or decomposition may be of relevance.

A compositional process to test-based risk assessment should follow the same steps as the (non-compositional) test-based risk assessment process. The main difference is that instead of assessing the system as a whole, it is decomposed into parts which can be assesses (more or less) as if each part were a whole system in itself. Figure 13 illustrates the case where the target of analysis has been decomposed into three parts which are each assessed using the same process for test based risk assessment that was described in Section 3.1. However, at certain points in the process, it may make sense to compose or decompose the assessment results before continuing with the rest of the process. In Figure 13, four such points are identified:

- After the first four steps of the assessment are completed, the resulting risk models may be composed into a single risk model which will be used as basis for test identification, selection, and prioritization. One of the reasons why this may be desirable is that this allows for a global prioritization of tests. If the test identification and prioritization is done for each risk model separately, then potential tests will not be compared across the risk models. For instance, it may be the case that one risk model results in the identification high-priority tests, while another results in low-priority tests, then low-priority tests might be selected for testing even though there are tests with higher priority in other risk models.
- After step 5.b of the process, test procedures (identified on the bases if the risk model(s)) may be composed or decomposed. One reason for this is that it might not make sense to decompose the test model in the same way as the target of analysis was decomposed prior to the risk assessment, or if the number of different test teams is different from the number of risk assessment teams.
- After step 6 of the process, when tests have been executed, the test results might be composed into a single model/document. Otherwise it may be difficult to validate the correctness of the risk model on the basis of the test results in the case where all test procedures were identified on the basis of a single risk model in the first place.
- After step 7 of the process, when the risk model(s) have been validated and treatments have been suggested, the resulting risk model may be composed into a global risk model to get an overview of all the risks that have been assessed.

In summary, we have identified four kinds of artifacts that may be composed or decomposed during the process: the *target of analysis*, the *risk model*, the *test procedures*, and the *test results*.

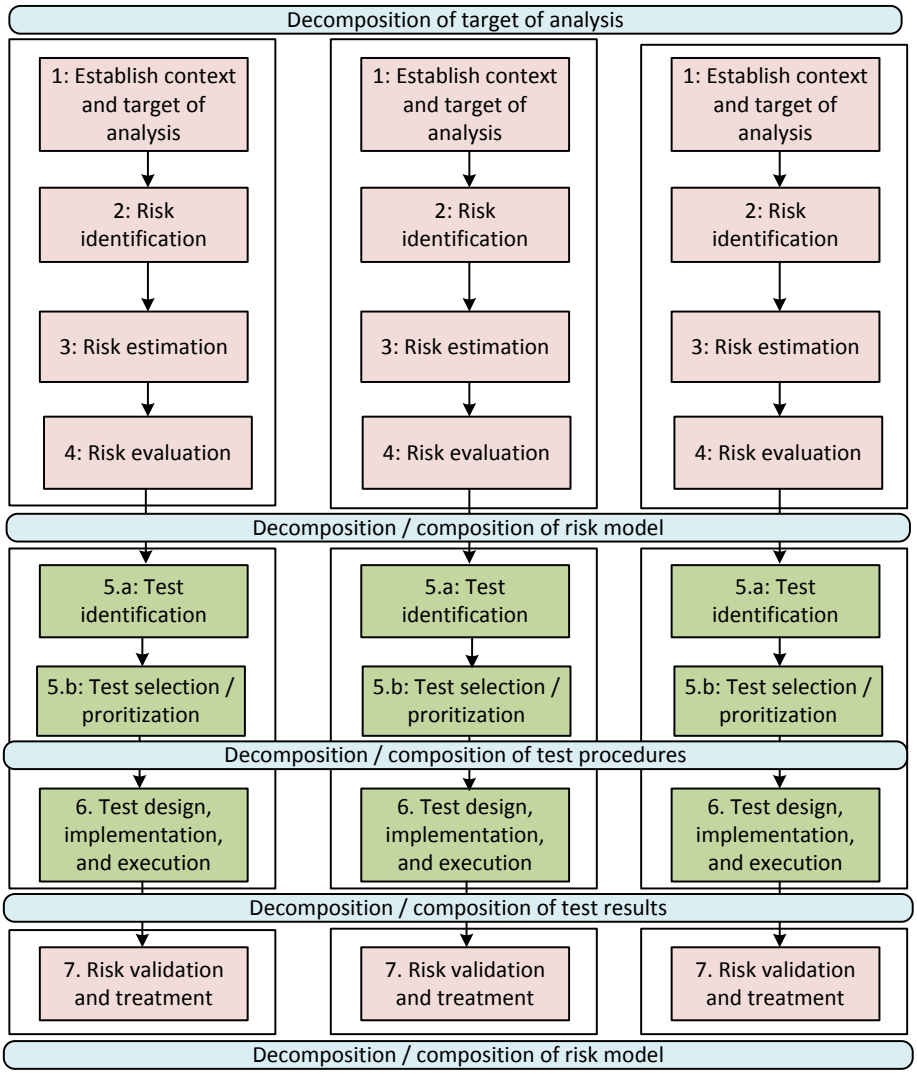

Figure 13 – Overview of a compositional test based risk assessment process

3.4 Legal Risk Assessment

In this section we describe a generic process for legal risk management and compliance management and how they could be aligned to achieve the RASEN objectives. Mahler [16] adopted the general risk management process described in Section 3.1 to fit to the management of legal risks. That section's description of the concepts within the risk management process remains applicable to this section. Figure 14 shows the methodology as tailored by Mahler [16] to fit the management of legal risks.

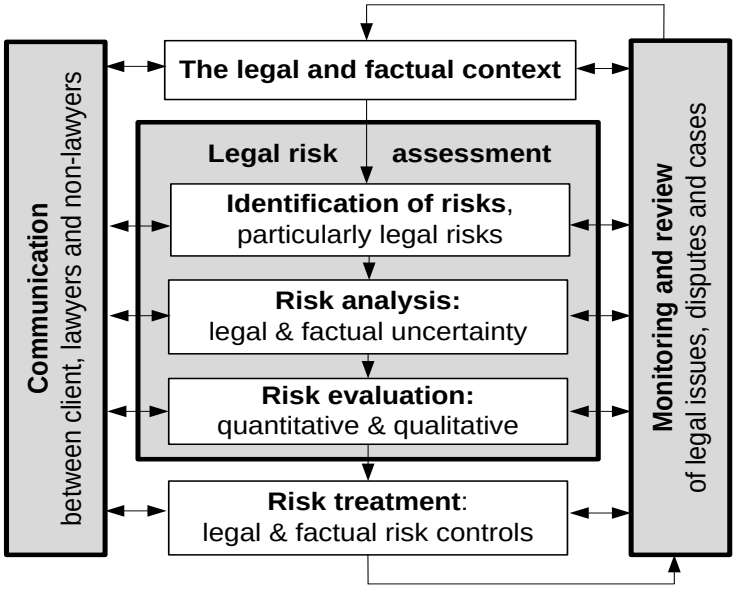

Figure 14 – Generic legal risk management process

As shown in the figure above, the management of legal risk involves one or more legal risk assessments. The deviation from the ISO 31000 concepts with regard to risk analysis noted above in Section 3.1 also applies to this section. Thus, a reference to legal risk analysis is used to denote the five step process in the middle of Figure 14 starting from the legal and factual context and ending with risk treatment.

The methodology developed by Mahler [16], although in line with the ISO 31000, lacks a specific focus on compliance management, which is of key importance for the RASEN project. The focus of legal risk management can be compliance risk management, structural risk management, contractual risk management and litigation risk management [16]. Contractual risk management focuses on the use of contracts with other entities outside the organization whereas compliance risk involves managing the risks of an organization resulting from legal obligations and prohibitions issued by different authorities [16]. Focusing on compliance may require certain risk management methods, which may differ from those appropriate if the focus is not compliance with existing norms, but rather designing new rules by formulating the clauses of a contract to be negotiated. The contract is designed to manage risks of another nature than deviation from the governing law. As a result, the methodology developed by Mahler, which focuses on contractual risk management, needs to be aligned as to enable the management of compliance related legal risks. One way of doing this would be to find some integration with existing compliance management processes. This way, it would also be possible to improve the existing compliance management processes.

One essential aspect which the existing compliance management methodologies lack is a risk-based approach to compliance (e.g. Solms 2005). Failure to take a risk-based approach could result in a somewhat low-key, 'tick the box' routine where organizations fail to assess their key risks [10]. When some kind of risk-assessment is involved, often, it forms part of an Enterprise Risk Management (ERM) standard such as COSO and does not stand as a distinct methodology. ERM normally focuses on risks for the enterprise as such (macro perspective), without necessarily assessing details at micro level, such as individual contracts, business relations, products or systems [16]. The alignment with the above ISO 31000 based legal risk management process is another factor of relevance. This is because the COSO framework possesses many technical and practical weaknesses, compared to the simpler ISO 31000 [16]. Standard documents and literature about enterprise risk management, and in particular the COSO model, do not address legal aspects in great detail [16]. Despite the fact that the Australian Standard for Compliance Program [1]refers to a risk assessment to be conducted, in the same way as its COSO counterpart, it does not specifically address risks resulting from legal uncertainty [16]. In addition, [1] does not provide a specific methodology for assessing compliance

risks. It rather offers a mix of processes, principles, strategies, and guidelines on how to achieve compliance. In fact, principle 3.1.g. of [1] points out the need for a comprehensive compliance process. Below we have identified the major compliance management processes from the Australian Standard that could be used as a baseline for RASEN. Figure 15 shows a compliance process based on the Australian Standard.

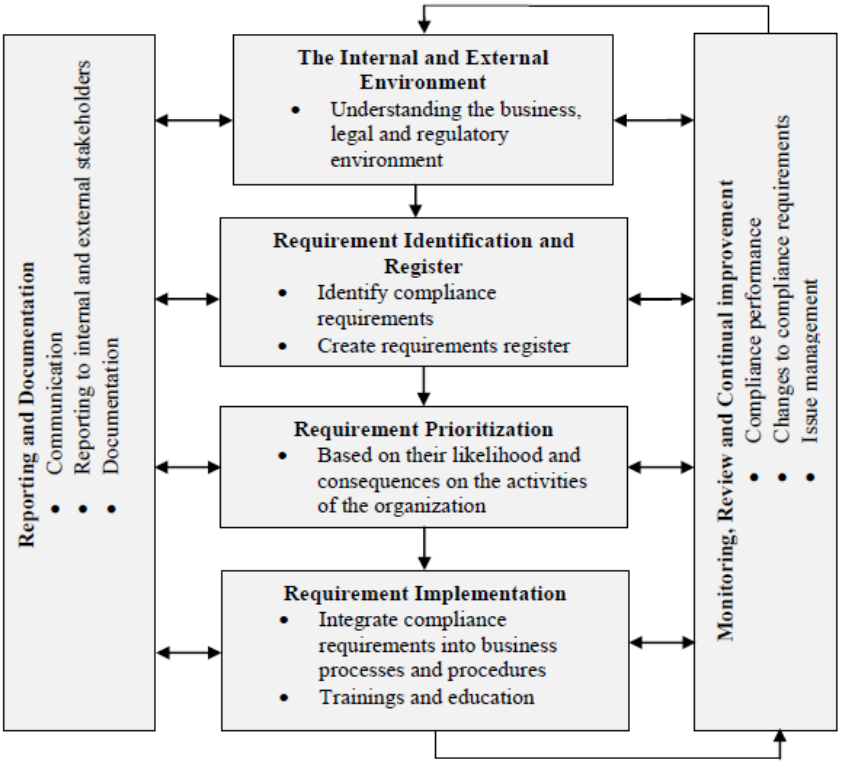

Figure 15 – Generic compliance management process

The Internal and external Environment – comprises understanding the environment under which the organization operates in, such as specific local or regional obligations and requirements, the organization's strategic objectives and values, the organization's structure and governance framework and the principles on which relationship with internal and external stakeholders are built [1]. It also includes developing a set of measurable indicators that will assist organizations in quantifying its compliance performance [1].

Requirement identification and register – a systematic identification of compliance obligations and prohibitions and the way in which they impact on the activities, products and services of the organization [1]. The key obligations and prohibitions under each of the compliance requirements will then be documented in a manner that is appropriate to its size, complexity, structure and operations in the forms, for example, a register, list or database [1].

Requirement prioritization – refers to the process of analyzing and ranking compliance requirements according to their impact on the operations of the organization and consequences of non-compliance [1]. An organization should identify compliance risks and rank their likelihood and consequences of potential failures [1].

Requirement implementation – putting control measures in place to manage the identified compliance obligations and prohibitions and achieve desired behaviors [1]. This includes, among other things, integrating compliance obligations into existing business practices and procedures including computer systems, forms, reporting systems and contracts [1]**.**

Monitoring, review and continual Improvement – involves ensuring that the compliance program and compliance performance are regularly monitored to ensure compliance performance is achieved [1]. Checking that compliance obligations are being met, reviewing the integrity and effectiveness of

the compliance program, checking the suitability, adequacy and effectiveness of controls at critical points [1]. The review should be followed by issue management where once an issue has been identified as a compliance failure or a potential failure; it should be reported, investigated, analyzed and classified to determine the cause and extent of required corrective and or preventive action required [1]. Corrective action should address the specific issue as well as a recurrence of compliance failures. Mechanisms that could be employed for checking and review include auditing, sampling and integrity testing, direct observation, formal interviews, facility tours and inspections [1].

Reporting and documentation – all actions taken in the process are documented, and relevant information is reported to internal and external stakeholders. Accurate, up-to-date records of the organization's compliance activities should be maintained to assist in the monitoring and review process and to demonstrate conformity with the program [1]. Accurate and complete information is provided to the correct people or areas of the organization to enable remedial action to be taken and employees should be encouraged to respond and report breaches of the law and other incidents of non-compliance [1]. The report might include issues on changes to compliance obligations, measurement of compliance performance, alleged breaches, corrective actions taken and evidence of effectiveness of actions, prioritization of the responses based on risk assessment, trainings given, results of reviews and audits [1]. Records should be stored in a manner that ensures they remain legible, readily identifiable and retrievable [1].

3.4.1 Towards an Integrated Approach to Legal Risk and Compliance Management

In this sub-section, we describe the potential benefits that the RASEN integrated approach to legal and compliance risk management could provide and how the integration would be achieved.

We have seen above that the methodology developed by Mahler needs to be aligned as to enable the management of compliance related legal risks whereas the compliance management process based on the Australian Standard lacks an adequate risk-based approach and has no space for specifically addressing risks resulting from legal uncertainty. Therefore, in RASEN we envisage a significant benefit coming from a methodology that would enable organization address legal risk and compliance management in an integrated manner. This way, the RASEN methodology will offer organizations the following important capabilities.

First, the integration between legal risk and compliance management opens up for testing compliance. This is because compliance management focuses not only on ensuring that controls are put in place but also checking the suitability, adequacy and effectiveness of controls at critical points and ensuring that undesirable conduct is not occurring [1]. This gives the possibility of using technical security testing to check compliance with legal norms of relevance to security. The objective within RASEN is begetting the technical security testing for checking compliance with security related legal norms. This is essential because checking compliance with information security obligations often involves checking the adequacy and effectiveness of the technological control measures. This could be done, for instance, by employing security requirements testing in order to validate the correct implementation of security requirements by testing the security functions. The risk-based testing described in Section 3.2 is relevant in this context as the results of the legal and compliance risk assessment could be used to prioritize compliance testing, based on the risk profile. The certifications for tested systems and documentations from the security risk analysis will also ease organizations' task of demonstrating compliance with the information security obligations.

Secondly, it will offer organizations the capability to manage their compliance and legal risks (including risks resulting from legal uncertainty) in an integrated and cost-effective way. This is achieved in two ways: through a risk-based approach and avoidance of unnecessary duplication of efforts. With regard to the former, the global scale of modern business has enabled companies to trade across borders but at the risk of being hauled to laws from diverse jurisdictions around the world. This is compounded by the introduction of myriad of new regulations following the corporate governance and compliance scandals associated with the recent financial crisis [19]. This has created an environment where meeting the requirements of a range of regulations, as well as internal policies and industry standards, is more important than ever. At the same time, as external expectations increase, so does the cost of compliance as companies allocate more people to risk and compliance management – consuming time and resources which could otherwise be used more productively in other revenue-producing

areas of the business [3]. Taking a risk-based approach toward compliance requirements enables them to focus resources on the most significant regulatory or legal issues facing their organizations [20]. Furthermore, both legal risk management and compliance management entail the identification of the legislation that needs to be complied with, implementing processes and controls to ensure adherence to the legislation, and monitoring and reporting on the implemented controls and processes [28].This entails a redundancy of unnecessary efforts if the tasks are kept in silos. With an integrated approach, it is possible to avoid such duplication of unnecessary effort, significantly reducing the number of people and the amount of time you need to be in compliance with regulations and manage your risks.

Finally, the integration would bring the methodology under the umbrella of an increasingly growing concept of integrated GRC approach. This is because apart from the compliance aspect, [1] adds some aspects of governance into the process. This begets organizations further advantages. Research shows that an integrated GRC platform brings better transparency in risk management, and creates competitive advantage by means of improved risk management [22]. This signifies that not only does the integrated approach offer a less costly methodology for companies but also turns the task of compliance and risk management into a competitive advantage. This fits well into the current ISO 31000 for risk management standard, which offers a more positive perspective towards risk management. It notes that risk management is not only the mitigation of loss, but also the improvement of "efficiency in operations, environmental protection, financial performance, corporate governance, human health and safety, product quality, *legal and regulatory compliance*, public acceptance, and reputation."

Having discussed the benefits of the integration, let us now turn to examine on how the integration could be achieved. In this regard, [17] underlines that integration does not mean 'consolidation' rather it means finding enhanced processes, common vocabulary and approach [30]. Accordingly, the table below seeks to find the interaction points and establish a common vocabulary that enables an integrated management of legal and compliance management.

Legal risk Management	**Compliance Management**	**Integrated legal risk and Compliance Management**
Establishing the legal and factual context	Understanding internal and external environment	Understand the business and regulatory environment
Establishing the legal and factual context	Requirement identification and register	Requirement and process identification
Legal risk assessment Risk identification Risk estimation Risk evaluation	Requirement prioritization	Legal and compliance risk assessment Risk identification Risk estimation Risk evaluation
Risk treatment	Requirements Implementation	Control Measures
Monitoring and review	Monitoring, review and continual improvement	Monitoring and review
Communication	Reporting and documentation	Reporting and communication

Table 2 – Integrating legal and compliance management processes

4 Initial RASEN Methodologies

In this section we describe initial RASEN methodologies. These methods can be seen as refinements of the generic baseline methods described in Section 3.

In Sections 4.1 and 4.2, we describe two alternative processes for test-based risk assessment. The first one mainly addresses test case derivation by use of patterns, while the latter mainly addresses the use of risk assessment for test procedure identification and selection/prioritization. In the final section, Section 4.3, we describe an initial method for legal risk assessment.

All the initial processes are documented in a similar manner. That is, each step of the methods are documented using the template shown in Table 3.

Name	**The name of the activity**
Actors	The actors that are referred to in the activity
Tools	The tools that are involved in the activity
Precondition	The precondition that need to be enabled when the activity is initiated.
Postcondition	The postcondition that describes the result of the activity.
Scenario	The scenario that describes the individual actions taken by the actors
Data exchanged/ processed	The data that are exchanged during the integration use case **In (from TOOL):** *The data that go into the activity. Terms from the conceptual model are used to describe the data.* **Out (from TOOL):** *The data that are the outcome of the activity. Terms from the conceptual model are used to describe the data.*

Table 3 – Template for documenting process activities

The possible actors and tools that can be referred to are described below.

Actors:

- **Customer:** The person/organization on whose behalf a security assessment is conducted.
- **Risk analyst:** The person responsible for doing the security risk assessment.
- **Security tester:** The person responsible for doing the security testing.
- **Compliance manager:** The person responsible for ensuring compliance.
- **Auditor:** The person responsible for auditing a system.

Tools:

- **Security risk assessment tool (SRAT):** The tool that supports the security risk assessment.
- **Security Testing Tool (STT):** The tool that supports the security testing.
- **Security Test Derivation Tool (STDT):** The tool that supports the derivation of test procedures and test cases from the SRAT tool to the STT tool.
- **Security test aggregation tool (STAT):**The tool that supports the aggregation of test results from the STT tool to the SRAT tool.

4.1 Initial RASEN Methodology for Test pattern supported risk based security testing

Test pattern based security testing combines the ideas of risk-based (security) testing (see Section 3.2), test-based risk assessment (see Section 3.1) with the idea of having reusable testing artefacts

called test pattern (see Sections 2.1, 2.2, and [31]). The following description mainly addresses the testing aspects of the methodology, since the risk assessment aspects are covered by the generic risk assessment methodologies that are the basis for test based risk assessment described in Section 2.2.

4.1.1 Overview

FOKUS and Smartesting introduce a risk-based security testing approach based on reusable security test patterns. The security test patterns are formalized by generic test purposes to provide a full automation of the testing process within the Model-Based approach proposed by Smartesting.The overall approach is depicted in Figure 16.

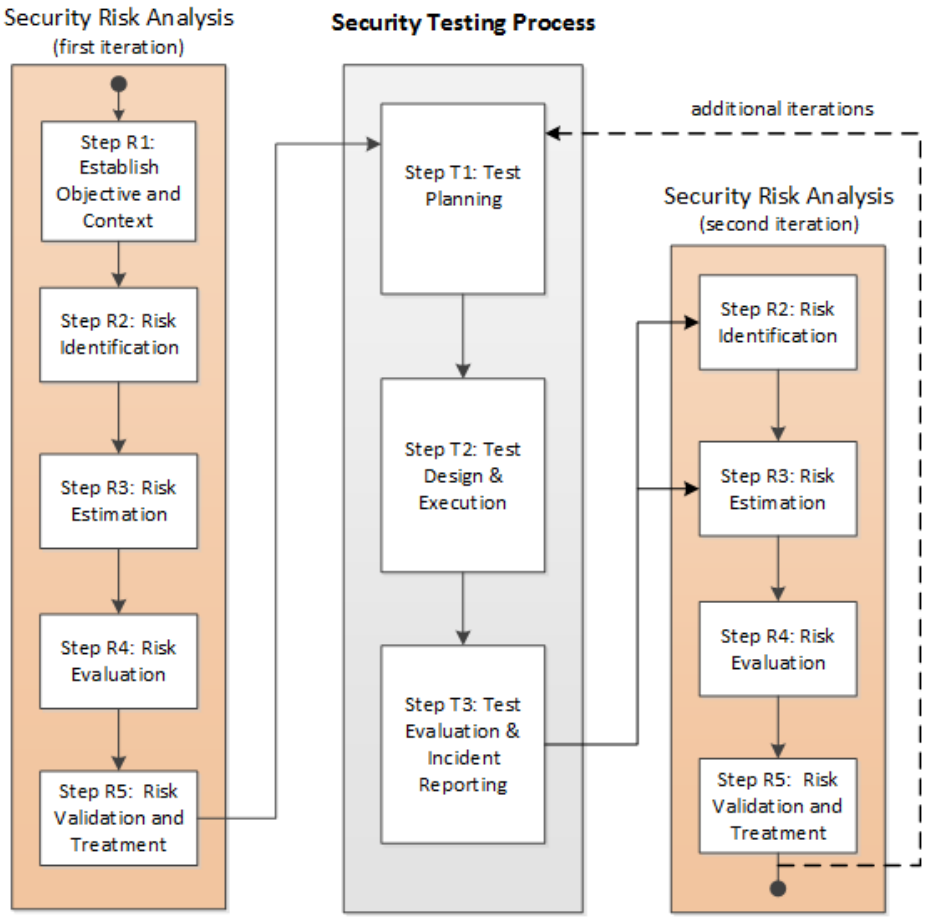

Figure 16 – Test-pattern supported risk-based security testing

The starting point for the overall methodology is a typical security risk assessment approach, which consists of the steps R1-R5 that are already defined in Section 3.1. The results of the security risk assessment are fed into the security testing process to support the test planning. This is similar to the integration of *Step2* in the generic risk based security testing methodology in Section 3.2. The security testing process is itself defined in three major steps (i.e. T1- T3) that distinguish test planning, test design & execution as well as test evaluation & incident reporting. While test planning (T3) is getting input from the risk assessment, the test evaluation & incident reporting provide the input for a second iteration of the risk assessment starting with the steps R2 or R3. In principle further iterations are possible by using the results of the second risk assessment iteration as input for a second testing iteration. In the following we provide a detailed description of the three major testing steps.

- **T1: Test planning:** From risk assessment (RA) to test patterns (TP)

- **Risk-based security test condition identification and prioritization:** Prioritize test items and test conditions on basis of the risk assessment (RA) and test patterns (TP(.
- **Risk-based security test technique identification and prioritization:** Maps security test patterns to threat scenarios or vulnerabilities (test coverage item identification, test technique identification & related test completion criteria)

- **T2: Test design and execution:** From test patterns to test implementation and execution
  - **Security test generation:** Generate test cases and test procedures(this process can be automated using Model-Based techniques)
  - **Security test execution and result determination:** Execute test procedures and determine test results and report test incidents
- **T3: Test evaluation and incident reporting:** From test results back to risk assessment
  - **Security test result aggregation:** Aggregate test results (e.g. by means of test and coverage metrics)
  - **Identify new threat scenarios and vulnerabilities (propagate results to R2):** Identify new threat scenarios and vulnerabilities by means of test incidents
  - **Adjust the risk assessment (propagate results to R3):** Adjust probability values and frequency values for vulnerabilities, threat scenarios, and unwanted incidents.

The following section provides a more precise specification of the individual activities of the methodology.

4.1.2 Process Description

Name	**Risk-based security test condition identification and prioritization**
Actors	Security Tester (ST)
Tools	Risk Assessment Tool (SRAT), Security Testing Tool (STT)
Precondition	A risk assessment model with likelihood and consequence estimates
Postcondition	A prioritized list of test conditions
Scenario	• ST identifies and prioritizes potential vulnerabilities and threat scenarios according to their impact on the overall risk picture. • ST assigns vulnerabilities and threat scenarios to features (interfaces, operations, components) of a test item. • ST tries to identify the vulnerabilities that have the highest impact when they are mitigated.
Data exchanged/ processed	**In (from SRAT):** *Vulnerabilities*, *threat scenarios*, *unwanted incident*, *likelihoods, consequences, risk level* **Out (from ST):** *Vulnerabilities* with *priority score*

Table 4 – Activity: Security risk-based test condition identification and prioritization

Name	**Risk-based security test technique identification and prioritization**
Actors	Security Tester (ST)
Tools	Security Testing Tool (STT)
Precondition	Vulnerabilities with associated test pattern (containing test technique, test completion criteria, test coverage item specification)
Postcondition	Vulnerabilities with priority score
Scenario	ST assigns vulnerabilities to test pattern (containing test technique, test completion criteria, test coverage item specification)
Data exchanged	**In :** *Vulnerabilities* with *priority score* **Out :** *Vulnerabilities* with associated *test pattern* and updated *priority score*

Table 5 – Activity: Security risk-based test technique identification and prioritization

Name	**Security test generation**
Actors	Security Tester (ST)
Tools	Security Testing Tool (STT)Security Testing Derivation Tool (STDT)
Precondition	*Vulnerabilities* with associated *test pattern* and updated *priority score*
Postcondition	*Test procedures* associated to *test pattern* and *vulnerabilities*
Scenario	ST generates/realizes *test cases* and *test procedures* according to the information given by the test pattern (test technique, test completion criteria, test coverage item specification).
Data exchanged	**In :** *Test pattern* and updated *priority score* **Out :** *Test procedures* and *test cases*

Table 6 – Activity: Security test generation

Name	**Model-Based Security test generation**
Actors	Security Tester (ST)
Tools	Security Testing Derivation Tool (STDT)
Precondition	*Vulnerabilities* with associated *test pattern* and *priority score* *Test purpose formalizing the vulnerability test patterns* *Behavioral/Environmental test model of the Application Under Test*
Postcondition	*Test cases and/or test procedures* associated to *test pattern* and *vulnerabilities*
Scenario	ST generates/realizes *test cases* and *test procedures* by automatically animating *the behavioral/environmental test model* according to the test purpose and priority score information (test technique, test completion criteria, test coverage item specification).
Data exchanged	**In :***Test pattern* and *priority score* **Out :***Test procedures* and *test cases*

Table 7 – Activity: Model-Based Security test generation

Name	**Security test execution and result determination**
Actors	Security Tester (ST)
Tools	Security Testing Tool (STT)
Precondition	*Test procedures* and *test cases*
Postcondition	*Test log* and *test incident report*
Scenario	ST executes *test procedures* and creates the *test log* and the *test incident report*.
Data exchanged	**In :** *Test procedures* and *test cases* **Out :** *Test log and test incident report*

Table 8 – Activity: Security test execution and result determination

Name	**Security test result aggregation**
Actors	Security Tester (ST),
Tools	Security Testing Tool (STT), Security Test Aggregation Tool (STAT)
Precondition	*Test log* and *test incident report* with associated *test procedures, test pattern* and *vulnerabilities.*
Postcondition	*Test results* are aggregated and displayed in the context of the associated *vulnerabilities*
Scenario	ST uses test and coverage metrics to assess the quality and meaningfulness of test results.
Data exchanged	**In (from STT):** *Test log* and *test incident report* with associated *test procedures, test pattern* and *vulnerabilities* **Out (to display and SRAT):** *Aggregated test results*

Table 9 – Activity: Security test result aggregation

Name	**Identify new threat scenarios and vulnerabilities**
Actors	Security Tester (ST), Security Testing Tool (STT), Security test aggregation tool (STAT)
Tools	
Precondition	*Test incident report with associated test log.*
Postcondition	*Vulnerabilities and threat scenarios to be added to the SRA*
Scenario	ST uses reported test incidents to identify new risks, vulnerabilities and threat scenarios to be added to the SRA.
Data exchanged	**In (from STT):** *Test log* and *test incident report* **Out (to SRAT manual process):** *Risks, vulnerabilities and threat scenarios*

Table 10 – Activity: Identify new threat scenarios and vulnerabilities

4.2 Initial RASEN Methodology for Test-Based Risk Assessment

In this section we describe a process for test-based risk assessment that mainly addresses the use of risk assessment for test procedure identification and prioritization/selection.

4.2.1 Overview

Figure 17 shows the main steps of the of the RASEN process for test-based risk assessment. The process is based on the generic process for test-based risk assessment (described in Section 3.1). The main differences are:

- Step 2 of the generic process has been removed.

- Step 6 of the generic process has been split into three steps: Test identification, Test selection/prioritization, and test design, implementation and execution.
- All the steps of the process related to risk assessment are based on the CORAS method for risk assessment [27].

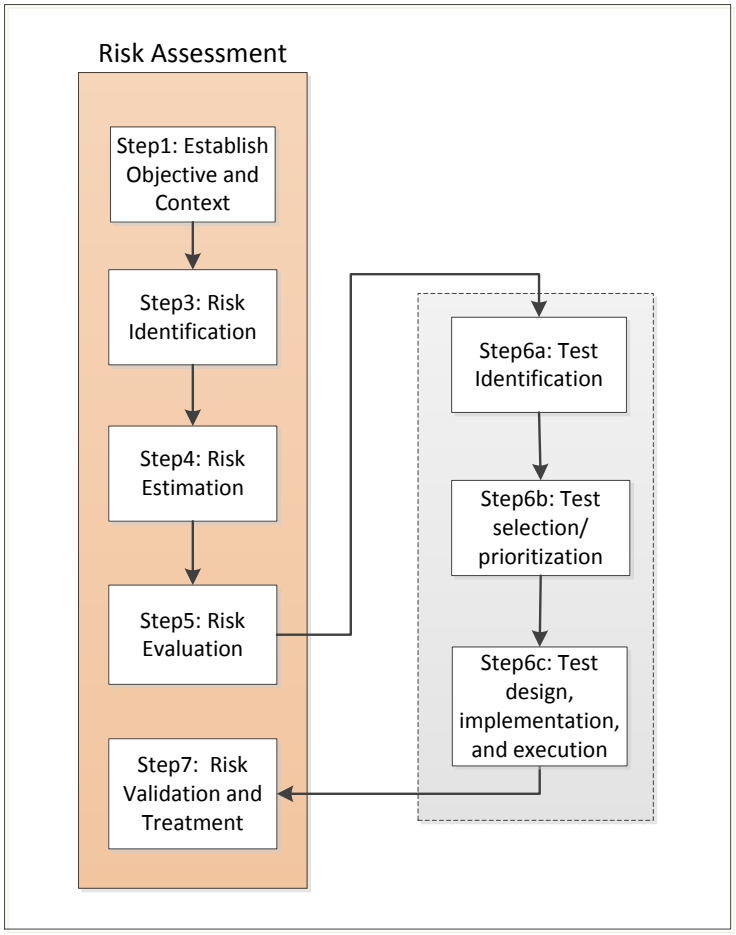

Figure 17 – Initial RASEN process for test-based risk assessment

In the following, we describe each step in more detail, and specifically highlight how the risk assessment steps of the process relate to the CORAS risk assessment method.

Step 1: Establish context and target of evaluation

Step 1 was carried out by performing the first four steps in the CORAS method:

- CORAS Step 1, preparation for the analysis, aims to make the necessary preparations for the actual analysis tasks based on a basic understanding of the target.
- CORAS Step 2, customer presentation of the target, aims to get the representatives of the customer to present their overall goals of the analysis, the target they wish to have analyzed, and the focus and scope of the analysis.
- CORAS Step 3, refining the target description using asset diagrams, aims to ensure a common understanding of the target of analysis by having the analysis team present their understanding of the target, including its focus, scope and main assets.
- CORAS Step 4, approval of target description, aims to ensure that the background documentation for the rest of the analysis, including the target, focus and scope is correct and complete as seen by the customer.

Step 3: Risk identification

Step 2 was carried out by performing the fifth step in the CORAS method:

- CORAS Step 5, risk identification using threat diagrams, aims to systematically identify threats, unwanted incidents, threat scenarios and vulnerabilities with respect to the identified assets.

Step 4: Risk estimation

Step 3 was carried out by performing the sixth and seventh step of the CORAS method:

- CORAS Step 6, risk estimation using threat diagrams, aims to determine the risk level of the risks that are represented by the identified unwanted incidents (discovered in CORAS step 5).
- CORAS Step 7, risk evaluation using risk diagrams, aims to clarify which of the identified risks are acceptable, and which of the risks must be further evaluated for possible treatment.

Step 6a: Test identification

The objective of the test identification activity is to identify potential test scenarios based on the CORAS threat diagrams that have been specified up to this point.

Step 6b: Test selection/prioritization

The purpose of the test selection/prioritization activity is to prioritize the identified potential test scenarios, and based on this, select the test scenarios that will developed further into concrete test cases.

Step 6c: Test design, implementation, and execution

The objective of activity 6 is to design, implement and execute test cases for each of the test scenarios and each vulnerability in the test scenarios that were selected in activity 5.

Step 7: Risk validation and treatment

The objectives of activity 7 are to (1) validate the risk model based on the test results and to update the risk model based on the test results (if necessary), (2) propose treatments for the most severe risks. The treatment process is based on the eighth and final step of the CORAS method.

- CORAS Step 8, risk treatment using treatment diagrams, aims to identify and analyze possible treatments for the unwanted incidents that have emerged. Treatments are assessed with respect to their cost-benefit evaluation, before a final treatment plan is made.

4.2.2 Process Description

In the following, we document each step of the process using the template described in Table 3.

Name	**Establish objective and context**
Actors	Risk analyst, Customer
Tools	Security risk assessment tool (SRAT)[the CORAS tool]
Precondition	None
Postcondition	The activity must end with the following output: • A description of the target of analysis, • A description of the assumptions, focus and scope of the analysis, • CORAS asset diagrams defining assets and parties, • Tables defining consequence and likelihood scales, and • Risk matrix tables defining risk evaluation criteria.
Scenario	• The Risk Analyst describes the target of analysis (for instance using UML) based on documentation that is already available and discussion with Customer. • The Risk Analyst documents assumptions, focus and scope of the analysis should be document in natural language in addition to the system documentation. • Based on discussion with the Customer, the Risk Analyst documents 1. assets and parties using CORAS asset diagrams using the Security Risk Assessment Tool; 2. at least one likelihood scale which will later be used when estimating the likelihood of risks; 3. one consequence scale for each identified asset which will later be used when estimating the consequences of risks; 4. risk evaluation criteria for each asset using a risk matrix.
Data exchanged/ processed	**Out (from CORAS tool):** Risk model with identified Assets

Table 11 – Activity: Establish objective and context

Name	**Risk identification**
Actors	Risk analyst, Customer
Tools	Security risk assessment tool (SRAT) [the CORAS tool]
Precondition	The precondition of this activity is the same as the postcondition of the activity "Establish objective and context"
Postcondition	The activity must end with the following output: • A set of CORAS threat diagrams
Scenario	• The Risk Analyst and the Customer walks through the target system description and identify unwanted incidents, threats, threat scenarios and vulnerabilities with regards to the assets that were identified in the activity "Establish objective and context". • The Risk Analyst documents the results using CORAS threat diagrams in the Security risk assessment tool.
Data exchanged/ processed	**In (from CORAS tool):** Risk model with identified Assets **Out (from CORAS tool):** Risk model with identified assets, threats, vulnerabilities, and unwanted incidents.

Table 12 – Activity: Risk identification

Name	**Risk estimation**
Actors	Risk analyst, Customer
Tools	Security risk assessment tool (SRAT) [the CORAS tool]
Precondition	The precondition for this activity is the same as the postcondition of the activity "Risk identification".
Postcondition	The activity must end with the following output: • A set of CORAS threat diagrams with likelihood and consequence values.
Scenario	• The Risk Analyst and the Customer walks through the risk model and estimate consequence values for unwanted incidents, and likelihood values for threat scenarios and unwanted incidents. • The Risk Analyst documents the results using CORAS threat diagrams in the Security risk assessment tool.
Data exchanged/ processed	**In (from CORAS tool):** Risk model with identified assets, threats, vulnerabilities, and unwanted incidents. **Out (from CORAS tool):** Risk model with estimated consequence values and likelihood values for threat scenarios and unwanted incidents.

Table 13 – Activity: Risk estimation

Name	**Risk evaluation**
Actors	Risk analyst, Customer
Tools	Security risk assessment tool (SRAT) [the CORAS tool]
Precondition	The precondition for this activity is the same as the postcondition of the activity "Risk estimation".
Postcondition	The activity must end with the following output: • A set of risk matrices containing all identified risks.
Scenario	• For each risk identified, the Risk Analyst plots the risk in the corresponding risk matrix according to the likelihood and the consequence values of the risk.
Data exchanged/ processed	**In (from CORAS tool):** Risk model with estimated consequence values and likelihood values for threat scenarios and unwanted incidents. **Out (from CORAS tool):** Risk model with risk matrices with risks.

Table 14 – Activity: Risk evaluation

Name	**Test identification**
Actors	Security tester
Tools	Test derivation tool (TDT) [the CORAS tool]
Precondition	The precondition for this activity is the same as the postcondition of the activity "Risk evaluation".
Postcondition	The activity must end with the following output: • A set of potential test procedures
Scenario	• The Security tester uses the TDT tool to generate a list of potential test procedures from the risk model.
Data exchanged/ processed	**In (from CORAS tool):** Risk model with risk matrices with risks. **Out (from CORAS tool):** A list of potential test procedures.

Table 15 – Activity: Test identification

Name	**Test selection/prioritization**
Actors	Security tester
Tools	Test derivation tool (TDT) [the CORAS tool]
Precondition	The precondition for this activity is the same as the postcondition of the activity "Test identification".
Postcondition	The activity must end with the following output: • A set of test procedures for deriving test cases
Scenario	• The secure tester uses the TDT tool to prioritize each potential test procedure. • The security tester uses the TDT tool to select those test procedures that have the highest priority and that will be the basis for test design. • The security tester exports the selected test procedures from the TDT tool to a list of test procedures described in natural language
Data exchanged/ processed	**In (from CORAS tool):** A list of potential test procedures. **Out (from CORAS tool):** A list of test procedures described in natural language to be used as a basis for test design.

Table 16 – Activity: Test selection/prioritization

Name	**Test design, implementation, and execution**
Actors	Security tester
Tools	Test Derivation Tool (TDT) [the CORAS tool], Security Testing Tool (STT) [any appropriate testing tool]
Precondition	The precondition for this activity is the same as the postcondition of the activity "Test selection/prioritization "
Postcondition	The activity must end with the following output: • Test results for each selected test procedure
Scenario	• For each test procedure, the security tester (manually) specifies concrete test cases. • The security tester executes the concrete test cases using the STT tool. • The security tester records the test results (manually) for each test procedure.
Data exchanged/ processed	**In (from CORAS tool):** A list of prioritized test procedures **Out (from STT)**: Test log, test incident report.

Table 17 – Activity: Test design, implementation, and execution

Name	**Risk validation and treatment**
Actors	Risk Analyst, Customer
Tools	Security risk assessment tool (SRAT) [the CORAS tool],Security test aggregation tool (STAT)
Precondition	The precondition for this activity is the same as the postcondition of the activity "Test selection/prioritization"
Postcondition	The activity must end with the following output: • An updated risk model (based on the test results) with suggested treatments.
Scenario	• The risk analyst imports the test procedures with associated test results into the STAT tool and aggregates the test results into measures that can be assess the impact that the results have on the risk model. • The risk analyst imports the test procedures with the high level test measures in to the SRAT tool which automatically calculates that impact that these results have on the risk model. • The risk analyst updates the risk model based on the impact assessment. • The risk analyst and the customer review the most severe risks and suggest treatments (if necessary) and document the results in CORAS treatment diagrams using the SRAT tool. • The risk analyst uses the SRAT tool to export the updated risk model with the treatments in a format that can be used in a risk assessment report.
Data exchanged/ processed	**In (from STT to STAT)**: Test log, test incident report. **Out (from STAT to CORAS tool):** Test procedures with high level test result measures. **Out (from CORAS tool):** An updated risk model (based on the test results) with suggested treatments in a format that can be used in a risk assessment report.

Table 18 – Activity: Risk validation and treatment

4.3 Initial RASEN Methodology for Legal Risk Assessment

4.3.1 Methodology for Legal and Compliance Risk Management: Overview

Figure 17 shows the main steps of the RASEN process for integrated legal and compliance risk assessment. The process is based on the integration of generic processes for legal risk assessment and compliance management described in Section 3.3. The main difference is:

- The addition of the check and react phase in Step 5, which is not visible in both generic processes above. The process of compliance checking and reacting is generally part of the monitoring aspect under both generic processes. Particularly, the continual improvement and issue management in the generic compliance management process specifically involve evaluating the suitability, adequacy and effectiveness of control measures followed by

necessary corrective actions. In RASEN we have opted to designate a distinct process step separate from monitoring and review. This comes from the desire to use security testing as a means to check compliance which is believed to contribute to the overall integration in the whole project.

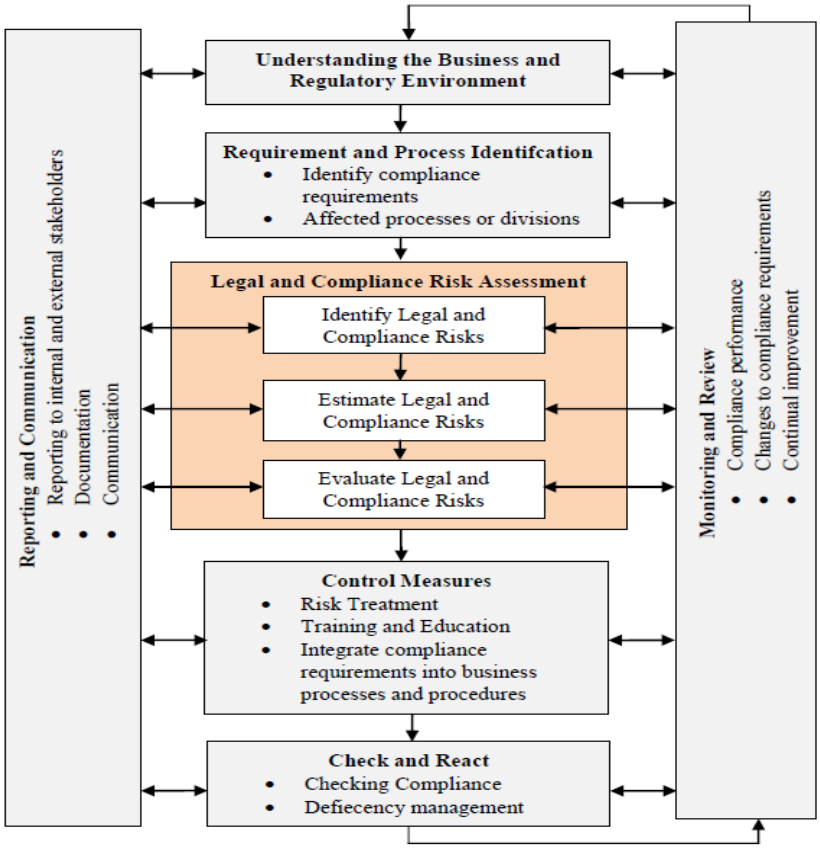

Figure 17 – Methodology for legal and compliance risk management

Steps

1. **Understanding business and regulatory environment**
    - Understanding the organizational objectives and structure
    - Defining the roles, responsibilities and timeline
    - Establish processes and boundaries within which organization operates:
        - Risk assessment criteria through tables defining consequence and likelihood scales
        - Risk matrix tables defining risk evaluation criteria.
        - Establish a commonly agreed set measurement, such as performance indicators
2. **Requirement and Process identification**
    - Identifying which law, regulation or standard the organization wants to comply with
    - Identify the divisions or processes in the organization that are affected by the requirements
3. **Legal and Compliance risk assessment**

- Identify legal and compliance risks
- Analyze all identified risks, assign value and estimate consequence
- Assign risk controls (accept or treat risks)

4. **Control measures**
   - Treat or mitigate risks
   - Place control measures in place to manage the identified compliance obligations and prohibitions
   - Integrate control measures into business process
   - Implement operating policies and procedures, work instruction manuals, system of recommendations and approval, segregation of duties, assigning competent employees
   - Relevant training and education
5. **Check and react**
   - Compliance testing(technical or non-technical)
   - Deficiency management

4.3.2 Process Description

Name	**Understanding Business and Regulatory environment**
Actors	Compliance Manager (CM), Risk analyst, customer
Tools	Risk Management Tool (SRMT), ARIS Business Architecture
Precondition	Decision to ensure compliance
Postcondition	The activity must end with the following output: • Organizational structure is modeled in SRMT • Tables defining consequence and likelihood scales, risk matrix tables defining risk evaluation criteria, and performance indicators documented in SRMT • Compliance policy that defines roles of actors, the time line for each activities
Scenario	1. **CM** models the organizational structure 2. **CM** documents the organizational structure and responsible people in **SRMT** 3. **CM** together with customer documents risk assessment criteria, performance indicators in **SRMT**
Data exchanged	**In (from stakeholder)** decision to ensure compliance **Data processed (in SRMT: ARIS Business Architecture):** risk assessment criteria, modeled organizational structure and responsible people

Table 19 – Activity: Understanding business and regulatory environment

Name	**Requirement and process identification**
Actors	Compliance Manager (CM), customer
Tools	Risk Management Tool (SRMT), ARIS Business Architecture
Precondition	The precondition for this activity is the same as the postcondition of the activity "Understanding business and regulatory environment"
Postcondition	The activity must end with the following output: • Processes under analysis is modeled in SRMT and responsibility attached to actors • Applicable legal requirements modeled in SRMT
Scenario	1. CM models applicable legal requirements in SRMT 2. CM models affected business process in SRMT
Data exchanged	**Data processed** (**in SRMT: ARIS Business Architecture):** Applicable compliance requirements**,** process under analysis

Table 20 – Activity: Requirement and process identification

Name	**Legal and compliance risk assessment**
Actors	Compliance Manager (CM), Risk Analyst (RA)
Tools	Risk Management Tool (SRMT), Risk Assessment Tool (SRAT),
Precondition	Models in SRMT: • Business processes under analysis • Applicable legal requirements • Risk assessment criteria and matrix
Postcondition	• Legal and compliance risks are identified • Risk value is assigned • Risk evaluation is carried out • Risk controls are assigned to risk
Scenario	1. RA and CM identifies legal and compliance risks 2. RA and CM uses SRAT to assign risk values to identified risks 3. RA and CM uses SRAT to evaluate risks 4. CM uses SRAT to assign risk controls to identified risks
Data exchanged	**In (from SRMT):** likelihoods and consequences, and risk matrix, business process under analysis, compliance requirements **Out (from SRAT, CORAS):** risk value, risk treatments

Table 21 – Activity: Legal and compliance risk assessment

Name	**Control measures**
Actors	Compliance Manager (CM)
Tools	Risk Management Tool (SRMT), Risk Assessment Tool (SRAT),
Precondition	• Identified risks are modeled in SRAT • Risk value is assessed in SRAT • Control measures are assigned
Postcondition	• Output of risk assessment (accept or treat risks) used to inform compliance process in SRMT • Control implemented business process model in SRMT
Scenario	1. Risk are imported into the SRMT 2. CM uses outputs from SRAT to model compliant business process in SRMT 3. Control measures are implemented into business processes and procedures
Data exchanged	**In (from SRAT: CORAS):** identified risks**,** risk value, risk treatments **Out (to SRMT: ARIS GRC):** control implemented business process model

Table 22 – Activity: Control measures

Name	**Check and react - Auditing test 1 (technical)**
Actors	Compliance Manager (CM), tester
Tools	Risk Management Tool (SRMT), STT ARIS GRC
Precondition	• Business process, risks and their controls are modeled in SRMT • Controls are implemented • Auditing test plan
Postcondition	Test result
Scenario	1. **CM** identifies system under test based on risk level and associated control measures 2. **CM** assigns responsibilities to tester 3. Tester establishes test cases 4. Tester executes test
Data exchanged	**In (from SRMT):** controls implemented business process model **Out (to STT):** Technical control measures (system under test), auditing test plan

Table 23 – Activity: Check and react - Auditing test 1 (technical)

Name	**Check and react- Auditing test 2 (non-technical)**
Actors	Compliance Manager (CM), tester
Tools	Risk Management Tool (SRMT), ARIS GRC
Precondition	• Auditing test plan • Business process, risks and their controls are modeled in SRMT • Controls are implemented
Postcondition	Test result
Scenario	1. CM identifies target of test, based on risk levels 2. CM assigns responsibilities to tester 3. Tester performs a test run
Data exchanged	**Data processed (in SRMT: ARIS GRC):** control process, business procedure under test, test results

Table 24 – Activity: Check and react - Auditing test 2 (non-technical)

Name	**Check and react- Deficiency management**
Actors	Compliance Manager (CM), tester
Tools	Risk Management Tool (SRMT), STT
Precondition	• Test results both from technical and non-technical • Business process, risks and their controls are modeled in SRMT
Postcondition	Corrective measures, test results linked into controls and business process
Scenario	1. **CM** imports testing results to the SRMT 2. **CM** analyses test results 3. **CM** recommends corrective actions
Data exchanged	**In (from SRMT: ARIS GRC, STT):** test results e.g. regarding their correct implementation, effectiveness **Out (to SRMT):** corrective actions

Table 25 – Activity: Check and react - Deficiency management

Demonstrating Compliance

Name	**Demonstrating Compliance**
Actors	Compliance Manager (CM), Auditor (internal or external),
Tools	Risk Management Tool (SRMT), ARIS GRC, ARIS Business Architecture
Precondition	• Business process, risks and their controls are documented in SRMT • Tests conducted and corrective measures taken are documented SRMT • Trainings and education given documented SRMT • Risks, controls and tests conducted are linked to BP and documented in SRMT
Postcondition	Checklist of risks identified, control measures taken, tests conducted and related corrective actions with clear link to business processes concerned
Scenario	1. Risks, controls, tests and corrective actions are attached to process and responsible people
Data exchanged	**In (from SRAT:ARIS GRC, ARIS Business Architecture, STT):** risk assessment results, controls placed, tests conducted and corrective measures taken **Out (Auditors):** Checklist of risks identified, control measures taken, tests conducted and related corrective actions with clear link to business processes concerned

Table 26 – Activity: Demonstrating compliance

5 Summary

In this document we have described a conceptual model for the RASEN methodologies, generic process that links the distinct domains addressed by RASEN, and initial RASEN methodologies that can be seen as refinements of the generic processes.

The conceptual model served as the starting point for the definition of the RASEN methodologies. It defined the central terms and their relationships within the domains of testing, security testing, risk assessment, security risk assessment, and legal risk assessment. The conceptual model has also served as a basis for the definition of the data model which will be used to integrate the RASEN tools.

The generic models defined in this document addressed the combination of risk assessment and testing, and also addressed the question where and why composition may be used in this setting. A generic model for legal risk assessment was also defined.

Finally the initial RASEN methodologies were presented in Section 4. Two of these addressed the combination of risk assessment and testing. One of them emphasized the use of patterns for the derivation of tests, whereas the other emphasized the use of the risk model for test identification, selection, and prioritization. Finally, the method for legal risk assessment addressed the integration of legal risk management and compliance.

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] 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.

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

[5] 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)

[6] ETSI: TTCN-3

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

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

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

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

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

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

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

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

[15] 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.

[16] Mahler, T.: Legal Risk Management: Developing and Evaluating Elements of a Method for

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

[18] 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

[19] Peterson E.A.: Compliance and ethics programs: Competitive advantage through law. Springer 2012, DOI 10.1007/s10997-012-9212-y.

[20] Ponemon Institute.:The Role of Governance, Risk Management & Compliance in Organizations,Study of GRC practitioners. (Ponemon Institute PLC, 2011)

[21] Racz, N., Weippl, E., Seufert, A.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In: De Decker, B., Schaumuller-Bichl, I. (eds.) CMS 2010, LNCS 6109, pp. 106–117. Springer (2010).

[22] Racz N., et al.: Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey among Large Enterprises. 21st Australasian Conference on Information Systems, Brisbane Dec 2010.

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

[24] 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)

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

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

[27] 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

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

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

[30] 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.

[31] RASEN Deliverable 4.3.1

[32] 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)

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

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