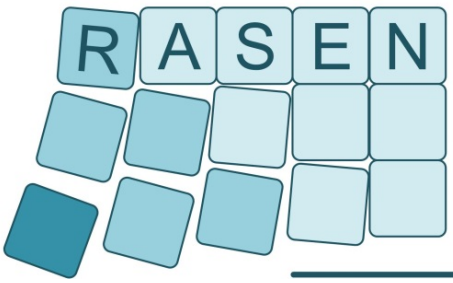

Compositional Risk Assessment and Security Testing of Networked Systems

The RASEN method for risk-based security testing and legal compliance assessment

Fredrik Seehusen[a] , **Jürgen Großmann**[b], **Samson Y. Esayas**[c]
[a]SINTEF ICT, [b]Fraunhofer FOKUS, [c]Dep. of Private Law, Univ. of Oslo

Managing cyber security has become increasingly important due to the growing interconnectivity of computerized systems and their use in society. A comprehensive assessment of cyber security can be challenging as its spans across different domains of knowledge and expertise. For instance, identifying cyber security vulnerabilities requires detailed technical expertise and knowledge, while the assessment of organizational impact and legal implications of cyber security incidents may require expertise and knowledge related to risk and legal compliance. We present a method that provides a comprehensive approach to cyber security by integrating three areas of cyber security assessment which are traditionally viewed in isolation: risk assessment, security testing, and legal compliance.

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

Motivating example:
A large organization develops and maintains ICT-products, and they have to ensure that these products are secure. This responsibility is split among many people with different roles in different departments: The *security testers* are responsible for identifying technical cyber security vulnerabilities. The *security managers* are responsible for ensuring that the products have an acceptable level of risk. The *legal compliance managers* are responsible for ensuring that the company meets its legal obligations. Although these roles are within different domains, there is a clear benefit of cross-domain collaboration. For instance, security managers and compliance managers may help the security testers to prioritize the testing based on impact on organizational assets, whereas security testers may help security mangers to assess the likelihood of the occurrence of security incidents and their technical impact.

The RASEN method addresses security risk assessments on different levels of abstraction and from different perspectives. Legal risk assessment especially addresses security threats in a legal context and under consideration of legal consequences.

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

Security risk assessment specifically deals with the assessment of security threats, their estimated likelihoods and their estimated consequences for a set of technical or business related assets. Finally, security testing can be used to actually examine the target of evaluation for vulnerabilities and its actual quality.

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

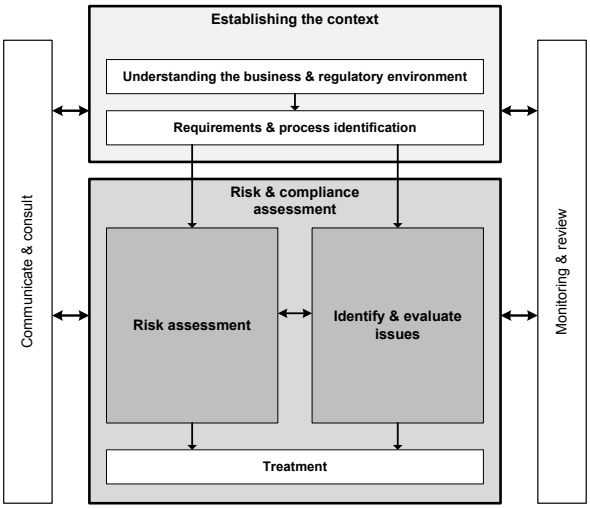

Figure 1 Overall risk, compliance and quality assessment process

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

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

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

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

Test-based risk assessment

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

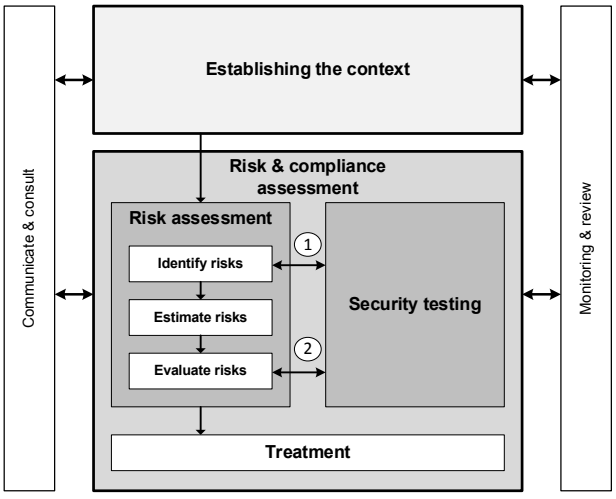

Figure 2 Generic process for test-based risk assessment

Figure 2 shows how the unified RASEN process is refined into a process for test-based risk assessment. Here the risk assessment activity has been decomposed into the three activities identify risks, estimate risks and evaluate risks. These three activities, together with the "establishing the context" and "treatment" activities form the core of

the ISO 31000 risk management process. As indicated in Figure 2, there are in particular two places where testing can in principle enhance the risk assessment process.

1. **Test-based risk identification:** In a risk assessment process, the risk identification activity is performed with respect to a target of analysis which is described and documented in the "establish context step". In a test-based risk assessment setting however, the risk identification is not only based on the documentation of the target of analysis, but also on relevant test results of target of analysis. Particularly relevant in this setting is testing using automated testing tools such as vulnerability scanners or network discovery tools.
2. **Test-based risk evaluation:** In a test-based risk assessment, the risk evaluation activity may be enhanced by test results (denoted (2) in Figure 2). At this point in the process, risks have already been identified and estimated, and the main reason for doing testing here is to gain increased confidence in the correctness of the risk model. In particular, the likelihood estimates of the risk model might have a low confidence if they e.g. depend on vulnerabilities whose presence in the target of analysis is unknown. By doing testing, we may investigate whether such vulnerabilities really are present in the target of analysis, and then use the test results to update the confidence level of the estimates of the risk model.

Risk-based security testing

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

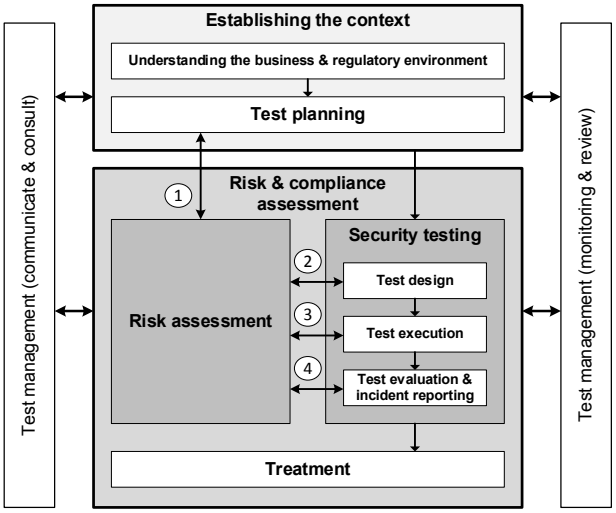

Figure 3 Generic process for risk-based security testing

Figure 3 shows the instantiation of the overall risk and compliance assessment process towards risk-based security testing. It consists of the classical phases of a testing process like it is specified in ISO 29119 and adds up to four additional activities, namely risk-based security test planning & management, risk-based security test design, risk-based security test selection, and security risk control. The activities are described in detail below.

1. **Risk-based security test planning:** The goal of risk-based security test planning is to systematically improve the testing process during the test-planning phase. Risk assessment is used to roughly identify high-risk areas or features of the system under test (SUT) and thus determine and optimize the respective test effort that is needed to verify the related security functionality or to address the related vulnerabilities. Moreover, a first assessment of the identified vulnerabilities and threat scenarios my help to select test strategies and techniques that are dedicated to deal with the most critical risks.
2. **Risk-based security test design and implementation**: During the test design and implementation phase, test cases are derived, implemented and assembled to test procedures. Security-risk assessment normally provides security threat and /or vulnerability models. These models contain qualitative information on expected threats and vulnerabilities for a

certain kind of application. This kind of information can be used to systematically determine what and how to test. It can be used to identify test condition (testable aspects of a system) as well as test purposes or high-level test scenarios that are dedicated to simulate potential threats and potential vulnerabilities that are not covered by the security functional requirements.

3. **Risk-based security test selection & execution**: Finding an optimal set of security test cases requires an appropriate selection strategy. Such a strategy takes the available test budget into account and also provides, as far as possible, the necessary test coverage. In functional testing, coverage is often described by the coverage of requirements or the coverage of model elements such as states, transitions or decisions. In risk-based testing coverage can be described in terms of risk model elements and estimates of their likelihoods and consequences. Risk-based security test selection criteria can be used to control the selection or the selected generation of test cases. The criteria are designed by taking the risks and their risk values to set priorities for the test selections, test case generation as well as for the order of test execution.
4. **Risk-based security test monitoring and control:** The decision on how extensive testing should be is always a question of the remaining test budget, the remaining time and the probability to discover even more critical errors, vulnerabilities or design flaws. The number of errors in the implementation hints at the maturity and provides a basis for assessing its security. In order to enable such an assessment, a sufficient degree of test coverage is required. Test results, test coverage information and a revised or affirmed risk assessment may provide a solid argument that can be used to effectively verify the level of security of a system.

While security test planning as well as security test monitoring and control belong to the test management process, security test design and implementation as well as security test selection and execution belong to the dynamic test process that is controlled by the test management process.

Risk-based compliance assessment

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

The RASEN method enables its users to prioritize compliance requirements based on their level of risks and to take account of legal consequences in making decision about security risks.

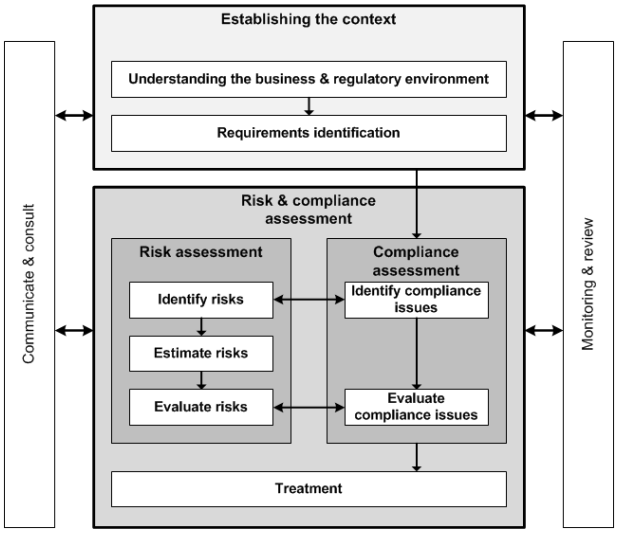

Figure 4 Integrated risk and compliance assessment

Figure 4 shows the RASEN method instantiated towards risk and compliance assessment. In the following, we describe the main interactions between compliance and risk assessment.

1. **Compliance risk identification:** The main goal of the compliance risk identification is to deal with compliance requirements that imply risk. The RASEN approach provides a structured method for identifying risks from compliance requirements or from the business environment. This also includes identifying legal consequences of technical security risks.

2. **Compliance risk estimation:** A risk with a large potential loss and a low likelihood of occurrence is often treated differently from one with a low potential loss and a high likelihood of occurrence. However, in order to estimate the risk, one needs to understand the underlying uncertainty. That uncertainty can originate from a number of sources, including from the compliance requirements themselves. For example, compliance requirements may be unclear, or there may be uncertainty about the consequences of noncompliance.

3. **Compliance risk evaluation:** The risk evaluation step is used to prioritize compliance requirements based on their level of risk and to prioritize security risks based on their legal consequences. Prioritization may be relevant to manage the treatment activities, for example, due to resource limitations.

Conclusion

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

The RASEN Project

The overall objective of the RASEN project is to strengthen European organizations' ability to conduct security assessments of large scale networked systems through the combination of security risk assessment and security testing, taking into account the context in which the system is used, such as liability, legal and organizational issues as well as technical issues.

Consortium

The RASEN project is coordinated by SINTEF ICT and consists of the following partners:

- **EVRY**, Norway (www.evry.no)
- **Fraunhofer FOKUS**, Germany (www.fokus.fraunhofer.de)
- **Department of Private Law**, University of Oslo, Norway (www.jus.uio.no/ifp)
- **Info World**, Romania (www.infoworld.ro)
- **SINTEF ICT**, Norway (www.sintef.no)
- **UFC/FEMTO-ST,** France (www.femto-st.fr)
- **Software AG**, Germany (www.softwareag.com)

Contact

Visit the RASEN website or contact us by email.

- www.rasenproject.eu
- rasen-web@list.modelbased.net

The project can also be followed on LinkedIn and Twitter.

- @RASENProject
- #RASENProject

www.linkedin.com/groups?home=&gid=7429037

Acknowledgments

The RASEN project (2012-2015) is funded by the European Commission via the Seventh Framework Programme, grant agreement no. 316853.

RASEN