RASEN
Compositional Risk Assessment and Security Testing of Networked Systems

Combining Compliance and Security Risk Assessment

Samson Y. Esayas[a], Tobias Mahler[a]
and Bjørnar Solhaug[b]
[a]Dep. of Private Law, Univ. of Oslo, [b]SINTEF ICT

Organizations that rely on ICT infrastructures need to maintain a high level of information security and protection from cyber-attacks. This is not only due to the self-interest of protecting business critical infrastructures; it is also due to laws that deal with information security. For this reason, technical and legal risks often need to be understood in combination. The RASEN project proposes an approach to integrate compliance and security risk assessment.

The prominence of information technology in day-to-day life means that businesses' ICT infrastructures attract great interest from both cyber-criminals and legislators. Businesses have to deal not only with the increased cyber-attacks, but also with an array of increasingly complex laws dealing with information security. Cyber-attacks clearly represent risks that businesses and organizations need to assess. The need to deal with these risks is based not only on the self-interest of the involved stakeholders, but is also reflected in legal and regulatory requirements. At the same time, some decisions based on legal requirements may also represent legal risks, for example in the form of possible sanctions. This complexity may require an integrated approach in order to jointly address legal and technical risks. The present paper describes the RASEN approach to the integration of compliance and security risk assessments.

Background

The global scale of modern business and information technology has enabled companies to trade across borders, but at the risk of being subject to laws from diverse jurisdictions. Regulatory fines for breach of security are becoming increasingly stringent. According to a Harvard Business Review survey, security and privacy have become significant areas of concern over the past few years.[1] According to the research, failure to deal with information security risks is not only costly in terms of finances and damage to the company and brand, but the regulatory penalties can also be quite large. This signifies the need for businesses to account for legal issues when addressing their information security risks and to ensure that their day-to-day business operations do not violate legal norms of relevance to information security, such as data privacy laws.

Moreover, several recent EU policy initiatives require risk management and have an impact on how risk assessment should be carried out. The proposed Network Information Services (NIS) Directive provides key requirements, and the proposed revisions to the Payment Services Directive (PSD2) are of particular relevance. In addition, the proposal for General Data Protection Regulation (GDPR) explicitly requires a controller, or where applicable the processor, to carry out a risk analysis on the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether the processing operations are likely to present specific risks.[2] These rules underline the paramount importance of con-

[1] A Report by Harvard Business Review Analytic Services: Meeting the Cyber Risk Challenge (2012)

[2] See for example Article 32(a) of draft General Data Protection Regulation and Article 14 of the NIS Directive

ducting a risk analysis both from legal and security perspectives.

Motivating Example and Challenges Addressed by RASEN

Example: A multi-national eHealth solution provider is investigating alternatives to scale up the flexibility of its ICT systems. As one of its strategies for addressing the problem, the company considers adopting cloud computing services. Given that its ICT systems are handling sensitive data of individuals, the company is uncertain of the viability of adopting cloud services due to the perceived compliance issues and security risks. As a result, the company starts to look at an approach that enables for assessing the associated compliance and security risks *vis-à-vis* the costs of their cloud proposal in a systematic way.

In the context described above, the technical decisions clearly imply legal risk, due to possible non-compliance with legal requirements. In particular, if the eHealth solution provider introduces cloud computing, there is a risk that governmental authorities can withdraw the necessary authorization in case of non-compliance. Similarly, compliance issues might affect the technical decisions. According to an opinion of the Article 29 Working Party,[3] cloud users have to undertake a comprehensive and thorough risk analysis. In this context they need to pay special attention to the legal risks regarding data protection, mainly security obligations and international transfers, before opting to go to the cloud.[4] However, the lack of a generally accepted methodology for legal risk management can represent a challenge.

Research has shown that the most important factor in the effective management of legal risks is having robust and clearly defined processes to evaluate risk on a continuous basis.[5] Such processes, the research emphasizes, must be specific to legal risk management and should enable better reporting, ensuring that critical risks are made visible to the right people as early as possible. Furthermore, in recent years the need for an integrated Governance, Risk and Compliance (GRC) management has gained significant prominence. According to one study, an integrated approach to GRC is not just desired but also "required" for complying with multi-source, evolving and complex regulations.[6] Despite the need for an integrated GRC approach, there have been hardly any specific methods or processes that enable the effective implementation of such an approach. This implies that providing a method that would enable for an integrated approach to risk and compliance assessments constitutes an essential contribution.

Furthermore, a particular challenge for assessing risks resulting from legal norms of relevance to information security, such as data privacy rules, is that the analysis often involves technical measures. The identification, assessment, and treatment of legal risks related to information security also rely on an understanding of the security risks and measures. Similarly, information security rules often prescribe security requirements that security risk analysts ought to heed. Lawyers, however, often lack the technical expertise needed to assess technical risks, and technical experts may lack detailed information about the legal security requirements and the legal consequences of technical problems. This requires an integrated approach that would enable to jointly address the technical and legal perspectives.

Technical decisions may imply legal risk and compliance issues may affect technical decisions.

The RASEN Approach – Integrating Security Risk and Compliance Assessments

The RASEN project addresses the above challenge by putting forth a systematic and risk-driven approach to risk and compliance assessments. By systematic we mean that relevant risks and control measures are mapped, to the extent possible, to

[3] This is a working group composed of national Data Protection Authorities.

[4] Article 29 Data Protection Working Party: Opinion 05/2012 on Cloud Computing (WP196) (2012)

[5] Practical Law Company: Benchmarking survey: Legal risk and compliance (2009)

[6] R. Bonazzi, L. Hussami, and Y. Pigneur: Compliance Management is Becoming a Major Issue in IS Design. A. D'Atri and D. Saccà (eds.), Information Systems: People, Organizations, Institutions, and Technologies, Springer Physica-Verlag Berlin Heidelberg (2010)

relevant compliance requirements. By risk-driven 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.

In the context addressed by RASEN in particular, the legal risk and compliance assessments will be integrated to the overall risk management framework, and will be carried out jointly with security risk assessment. The main objective of the integration is to enable the following:

- The security risk assessment takes account of the legal and compliance issues where the legal risk analysis might help to prioritize the treatment of security risks.
- The legal and compliance assessment benefits from the security risk assessment. For example, the security risks can be used as an input for legal risk assessment and support a systematic approach to legal compliance.
- The security risk assessment provides information relevant for compliance with breach notification requirements.

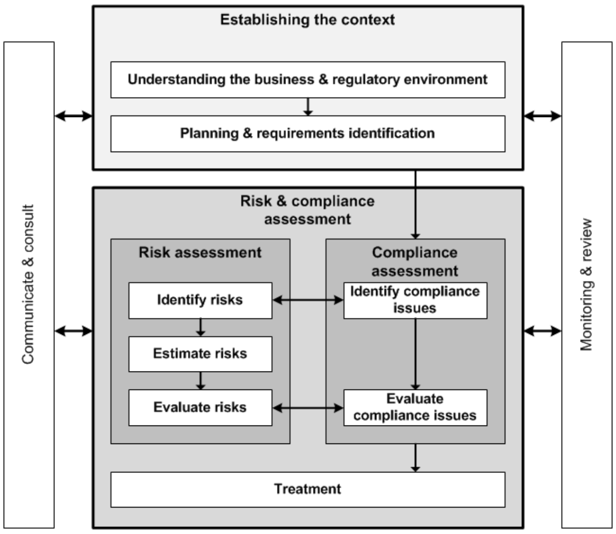
Establishing the context
Understanding the business & regulatory environment
Planning & requirements identification
Communicate & consult
Monitoring & review
Risk & compliance assessment
Risk assessment
Identify risks
Estimate risks
Evaluate risks
Compliance assessment
Identify compliance issues
Evaluate compliance issues
Treatment

Figure 1 – Integrated risk and compliance assessment

Figure 1 shows the overall risk and compliance assessment process. It consists of the risk assessment process as specified in ISO 31000 and a generic compliance assessment process derived from the Australian Standard for Compliance Programs (AS 3806-2006)[7]. In the following paragraphs, we describe the two main interactions between compliance and risk assessment.

1. **Compliance risk identification:** Once the context is established, risks can be identified. The main goal of the compliance risk identification is to deal with compliance requirements that imply risk. The RASEN approach provides a structured method for identifying risks from compliance requirements or from the business environment. This should also include identifying legal consequences of security risks.
2. **Compliance risk estimation:** Risk with a large potential loss and a low probability 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 non-compliance.
3. **Compliance risk evaluation:** The risk evaluation step is used to prioritize compliance requirements based on their level of risk and to prioritize security risks based on their legal consequences. Prioritization may be relevant, for example, due to resource limitations.
4. **Treatment:** The goal of this step is to allocate compliance resources efficiently based on their risk level as well as any relevant ethical issues. Once implemented, the measures will contribute to achieving compliance with legal norms, including those relevant to security. In order to avoid unethical business conduct, the risk-based compliance measures should also take consideration of ethical issues. Checking compliance (auditing) also benefits from the risk-driven approach where only high risks areas are audited or checked. In addition, decisions regarding security risks would take account of the legal consequences of security risks.

[7] Australian Standard 3806-2006, Compliance programs (2006)

Conclusion

The integration between risk assessment and compliance in general envisions two major goals. First, it aims at risk-based compliance where the risk assessment is used to deal with compliance requirements that imply risk. Second, it aims at using the risk assessment and its results to support systematic compliance with legal norms of relevance to security. Such an approach enables the method user to prioritize compliance requirements based on their level of risks and to take account of legal consequences in making decision about security risks.

By linking security risk assessment to legal and compliance issues, the approach gives organizations a holistic picture of how the organizations' risks (legal and technical), controls, and compliance requirements interact.

The RASEN Project

The main 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)
- **Smartesting**, France (www.smartesting.com)
- **Software AG**, Germany (www.softwareag.com)

Contact

Visit the RASEN website or contact us by email.

- www.rasenproject.eu
- contact@rasenproject.eu

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.