2014 IEEE International Symposium on Software Reliability Engineering Workshops

Structuring Compliance Risk Identification Using the CORAS Approach: Compliance as an Asset

Samson Yoseph Esayas
Norwegian Research Center for Computers and Law, University of Oslo
Oslo, Norway
s.y.esayas@jus.uio.no

Abstract—**The global scale of modern business and information technology enables companies to trade across borders but at the risk of being subject to laws in diverse jurisdictions. The regulatory requirements with which businesses have to comply are drastically increasing not only in sheer number but also in complexity, confronting businesses with the need to adapt to a complex, evolving regulatory environment. Crucial to a business's survival and profitability in such environment are understanding and managing legal and compliance risks. This need has spurred significant recent interest in integrated governance, risk, and compliance (GRC) management. A central element in integrated GRC management is following a risk-based approach to compliance which prioritizes compliance requirements based on their level of risk. Despite the need for risk-based compliance, few specific methods or approaches for identifying compliance risks have been developed. This paper presents a structured method for identifying compliance risks from compliance requirements and the business environment.**

Index Terms*—*Compliance, risk identification, legal risk, compliance management, risk management.

I. Introduction

THE INCREASED business opportunities resulting from globalization and recent corporate governance and compliance scandals have led to the introduction of many new business regulations [1]. Laws and standards are not only drastically increasing but are also becoming more complex and sometimes contradictory [2]. These changes have led to higher compliance costs 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 businesses. Organizations are finding complying with numerous regulations to be very expensive [3]. Thus, identifying compliance challenges early and understanding the specific non-compliance risks in order to prioritize compliance requirements has become essential. This need has led to growing recent interest in organizations' governance, risk, and compliance (GRC) activities.

Research shows that an integrated approach to GRC is not only desirable but also necessary to comply with evolving, complex regulations from multiple sources [4]. An integrated GRC approach avoids duplication of efforts, significantly reducing the people and time devoted to complying with regulations and managing risks [5]. The legal environment, thus, plays a pivotal role in driving interest in GRC. Studies show that regulatory compliance is the main driver of GRC [5][3]. Similarly, more legal and regulatory requirements are cited as the main factor triggering risk management, and companies are less willing to accept risks resulting from law as compared to perational, and business risks [6]. The higher importance of compliance risks raises the need to explore methods for structuring the identification of compliance risks.

Sometimes, the need to proactively identify compliance risks emerges not only from the self-interest of the involved stakeholders but also from legal and regulatory requirements. For example, proposed European Union (EU) General Data Protection Regulation [6] explicitly requires a controller or, where applicable, a processor to carry out a risk analysis of 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 (for example, see Article 32(a)). These rules underline the paramount importance of such risk analysis of data subjects' rights and freedoms when the processing involves special categories of personal data, such as health data. Similarly, in the opinion of the Article 29 Working Party,[1] cloud users should perform comprehensive, thorough risk analysis. They need to pay special attention to the legal risks regarding data protection, primarily security obligations and international transfers, before opting to go to the cloud [8]. However, the European Data Protection Supervisor has criticized the lack of specific guidelines for how to conduct such legal risk analysis and has recommended that the European Commission develop templates for evaluating and managing risks in cloud computing [9]. Although the European Network and Information Security Agency (ENISA) [10] has provided some guidelines on cloud computing risk assessment, including legal risks, there is no specific guideline for identifying legal risks.

Different international standards provide guidelines for managing compliance. Prominent among such standards are the Australian Standard on Compliance Program [11] and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) [12]. An essential feature which existing compliance management methodologies lack is a risk-based approach to compliance [13]. Failure to take a risk-based approach could result in a low-key, tick-the-box routine in which organizations fail to assess their key risks [14]. When a risk assessment is undertaken, it often is part of an enterprise risk management (ERM) standard, such as COSO, and is not a

[1] This is a working group composed of national data protection authorities.

978-1-4799-7377-4/14 $31.00 © 2014 IEEE
DOI 10.1109/ISSREW.2014.67

distinct methodology [15]. Although the Australian Standard on Compliance Program and its COSO counterpart call for conducting compliance risk assessment, they do not provide a method or approach to identify legal and compliance risks. Therefore, providing a method to help structure and simplify compliance risk identification stands as an essential contribution. This paper presents a structured method for identifying compliance risks from compliance requirements and the business environment.

II. Understanding Compliance

Compliance is defined as adhering to the requirements of legal, industry, and organizational standards and codes, to principles of good governance, and to accepted community and ethical standards [11]. Compliance occurs when businesses or individuals take action to ensure adherence to various requirements. Compliance requirements come from many sources, legal and non-legal. Legal sources include legal regulations, contracts, and court decisions, while non-legal sources are industry and organizational standards and codes, principles of good governance, and accepted community and ethical standards.

The modality of compliance requirements from compliance sources can take the form of obligations, permissions, and prohibitions. In addition to stipulating rights, obligations, and prohibitions, compliance texts contain explanatory norms, such as definitions of terms and exceptions, which refine, add, or constrain the other modalities. Although understanding such terms is essential, the focus of compliance is mostly on obligations and prohibitions because they compel or restrict actors from doing certain things. Obligation norms prescribe the specific actions that an organization must undertake, and prohibition norms stipulate the actions that an organization must avoid in order to comply with a given compliance requirement. As well, obligations and prohibitions are often attached to consequences, which can be sources of risks. This means, failure to perform the obliged activity and performance of the prohibited activity affects the compliance. From a risk management perspective, failure to adhere to compliance requirements constitutes a source of risk which ought to be managed. Managing compliance risks involves a series of steps, such as identifying and assessing non-compliance risks and then applying appropriate compliance measures to control them.

The benefits of risk-based compliance include enabling the allocation of resources to the areas where they are most needed based on risk levels. Targeting compliance measures to the most important risks ensures that resources are concentrated in the areas where they can most improve compliance outcomes. Second, risk-based compliance improves business support for compliance measures because risk management processes are widely understood within the business [16]. In addition, it opens a door for a risk-driven auditing or compliance checking which assesses only high-risk areas and better uses resources. However, as mentioned, there are few techniques for identifying compliance risks in a structured manner. This proposed structured approach aims at simplifying the identification of compliance risks by schematically translating compliance requirements into the notions of threat scenarios and unwanted incidents used in the CORAS risk analysis approach. However, the structured approach can also be implemented using other notations for risk modeling.

III. The CORAS Approach

CORAS is a risk analysis approach consisting of three main artifacts: (1) a customized diagrammatical language for risk modeling; (2) a tool supporting the language; and (3) a method for asset-driven risk analysis [17]. The artifacts relevant to this paper are the CORAS language and tool. The CORAS language covers notions, such as threats, vulnerabilities, risks, unwanted incidents, threat scenarios, and assets, and aims to facilitate communication among participants with different backgrounds [17]. The CORAS tool supports the notions within the language with easy-to-understand icons (symbols). The tool enables communication among experts from different disciplines and the documentation of risk assessment results. Fig. 1 shows the CORAS notions and their graphical representations.

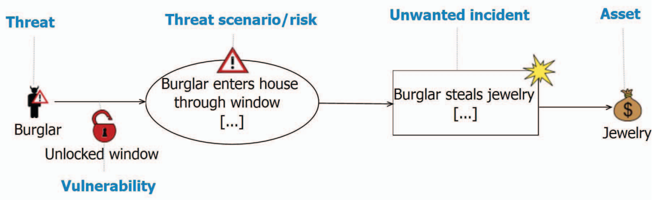

Fig. 1. CORAS notions and their graphical representation.

In [18], the authors examine the possibility of specifying legal threat scenarios using the CORAS threat diagram. More extensive work by [17] shows that the CORAS tool can be used to model legal risks. However, the CORAS approach offers little help on how to identify compliance risks. This paper builds on the previous works by mapping the CORAS notions to compliance requirements in order to systematically identify compliance risks from requirements.

IV. Identifying compliance risks

Central to the risk-based approach to compliance is the identification of the risks of non-compliance. Failure to properly consider risks can lead to the selection of inappropriate compliance measures and ineffective regulatory outcomes. According to ISO31000 [19], the key aspects of risk identification are the sources of risk and events. In the context of compliance, risk identification involves examining how a compliance requirement—an obligation or prohibition—can lead to risk. Among the available risk identification techniques, structured brainstorming is considered relatively well suited for the compliance context because it involves an interdisciplinary group of experts [15]. In brainstorming activities, different stakeholders contribute their knowledge and experience to identifying risk events and assessing these events under the law, guided by structured questions. In the context of compliance, risks can be identified using two approaches: *law centered* and *facts centered* [15]. At the core of the law-centered approach is the compliance norm or requirement. In this approach, the brainstorming activity focuses on identifying, through guiding questions, what triggers this norm. When applied to voluntary compliance requirements, this approach can be described as *requirement centered*. In contrast, the *facts-centered* approach focuses on identifying facts and assessing their compliance implications. The facts-centered approach also reuses already identified risks from other areas, such as technical risk assessments, and assesses their compliance implications. The law and factual assessments need to be understood together in order to get a full picture of the legal or compliance risk.

A. Requirements-Centered Approach

In the requirements-centered approach, the goal is to identify risks by focusing on the compliance requirement, such as an obligation or prohibition. Every compliance norm consists of an antecedent (if A) and a consequent (then B) [20]. The antecedent is the circumstances necessary for the norm to apply. The consequent is the (legal) effects of the application of the norm. The (legal) effect of a particular norm depends on the factual circumstances: an actor, an activity performed by that actor on a target, and the actor's role while performing that activity (see TABLE 1 for an example). This implies that the 'activity' performed by an 'actor' in a certain 'role' should be in-line with the 'activity' prescribed by the compliance requirement. Fig. 2 shows the conceptual model for a compliance norm.

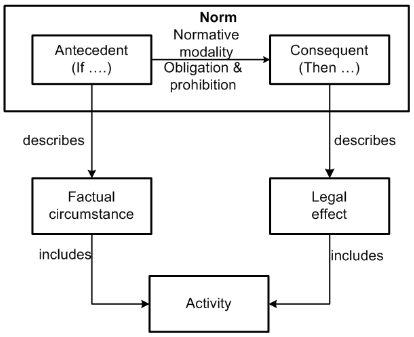

Fig. 2. Compliance norm

These concepts of the compliance norm can be mapped to the concepts of risk analysis used in the CORAS approach, as shown in Fig. 3.

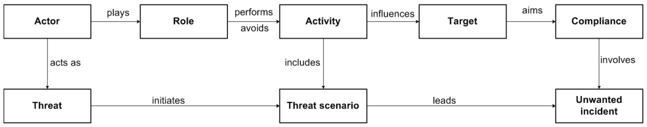

Fig. 3. Mapping compliance norm to CORAS notions.

While identifying compliance risks in the requirement-centered approach, the focus is on the 'activity' which is obliged or prohibited. If the activity is an obligation, then the threat scenario is failure to perform that specific activity. If the activity is a prohibition, the threat scenario is the possible performance of that specific 'activity'. In addition, the threat scenario must lead to non-compliance with the specific compliance norm in order to become an unwanted incident, causing deviation from the objective or asset. Not all failures to perform an obligation or performances of a prohibited activity lead to non-compliance. For example, an actor might be generally prohibited from doing a certain activity but may do it under certain circumstances. Considering such exceptions, the unwanted incident can be schematically translated from the legal source as non-compliance with the specific compliance source, as shown in Fig. 4.

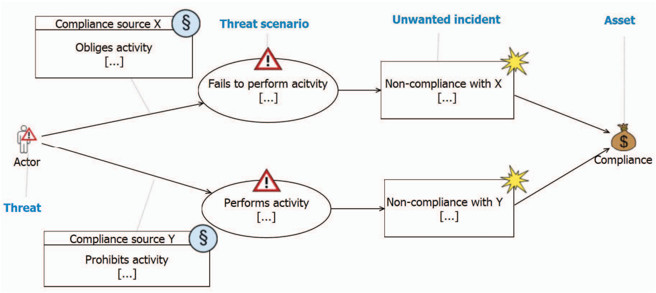

Fig. 4. Modeling compliance threat in CORAS.

B. Facts-Centered Approach

As briefly noted, the facts-centered approach identifies risks by focusing on the facts or other risks and assesses their compliance implications. This approach is especially relevant in the context of information security because of the capability to assess the compliance implications of security risks [21]. The alignment of compliance and security risk analysis enables accounting for legal requirements in risk-decision making. This ensures that a risk considered acceptable by the organization's criteria is acceptable from that organization's legal position. Generally, the facts-centered approach aids in assessing the compliance implications of a planned change, project, or task.

In the facts-centered approach, the stakeholder is aware of certain facts or risks and wishes to consider their compliance implications. Once the facts are known, all compliance requirements which might be triggered are identified through guiding questions. Next, the risks of non-compliance are identified in the same manner as in the requirement-centered approach by focusing on the notion of activity presented in the compliance requirement.

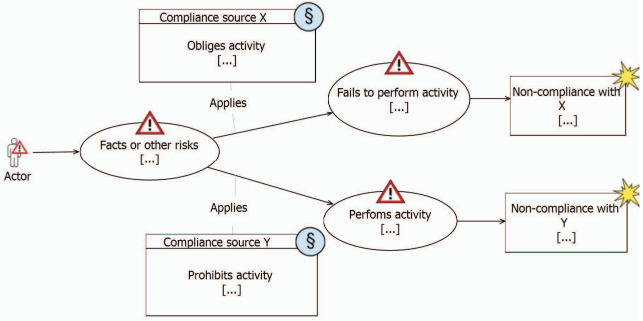

Fig. 5. Facts-centered CORAS threat diagram.

V. Structured Compliance Risk Identification

The identification of legal and compliance risks involves substantial amount of analytical activity, and can be time consuming.[2] The main goal of this proposed approach is to reduce the effort involved in identifying legal and compliance risks by structuring the identification of compliance risks. This is achieved by providing the risk analyst with a starting point for risk analysis by schematically translating the compliance requirements and facts in the business environment into threat scenarios and unwanted incidents. These artifacts can be used for further analysis during brainstorming sessions and meetings with stakeholders. Doing so may reduce the time spent conducting legal and compliance risk analysis.

In the requirement-centered approach, the starting point is a compliance requirement. Here, I illustrate the structured approach for identifying legal and compliance risks using a provision taken from Norwegian ICT regulation.[3] The regulation primarily concerns the ICT system of financial institutions, such as banks. Section 13 of the regulation, entitled "Documentation," stipulates the following:

> *An assembled up-to-date overview shall exist of the organization, equipment, systems and significant factors related to ICT activities. An up-to-date documentation shall exist of each ICT system important to the institution which document the compliance with the demands in this regulation.*

Once the compliance requirement is identified, the determination of possible non-compliance risks can begin by identifying the notions of the actor, the normative modality, and the activity the actor is obliged to or prohibited from performing. For example, Table 1 can serve as a starting point for structuring a requirement into these notions.

TABLE 1. TEMPLATE FOR STRUCTURING COMPLIANCE RISK IDENTIFICATION

Legal source	ICT Regulation Section 13
Modality	Obligation
Actor	Bank
Role	ICT system owner
Activity	An assembled up-to-date overview shall exist of the organization, equipment, systems, and significant factors related to ICT activities. Up-to-date documentation shall exist of each ICT system important to the institution which documents compliance with the demands in this regulation.
Target	ICT system
Threat scenarios	Failure to document an up-to-date overview of the organization, equipment, systems, and significant factors related to ICT activities Failure to keep up-to-date documentation of important ICT systems and their compliance with the regulation

In the preceding example, the set of activities in Section 13 which the bank is obliged to perform are schematically translated into threat scenarios by adding failure to perform in front of the activity. The unwanted incident is identified by adding non-compliance to the compliance norm at hand. This can be translated into a CORAS diagram as follows.

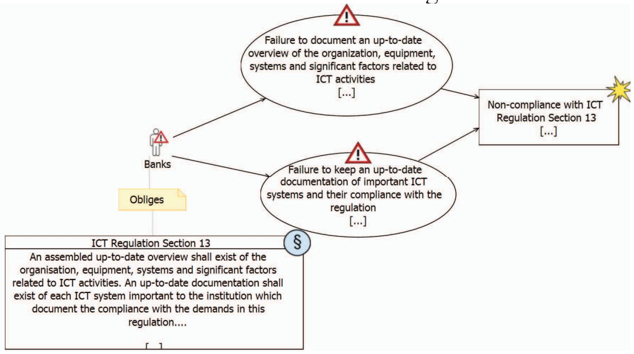
Failure to document an up-to-date overview of the organization, equipment, systems and significant factors related to ICT activities
[...]
Non-compliance with ICT Regulation Section 13
[...]
Banks
Failure to keep an up-to-date documentation of important ICT systems and their compliance with the regulation
[...]
Obliges
ICT Regulation Section 13
§
An assembled up-to-date overview shall exist of the organisation, equipment, systems and significant factors related to ICT activities. An up-to-date documentation shall exist of each ICT system important to the institution which document the compliance with the demands in this regulation....
[...]

Fig. 6. CORAS compliance threat diagram.

The risk analyst can prepare the template in TABLE 1 and Fig. 6 either in advance or during the brainstorming activity with the relevant stakeholders. The prepared template can be used to initiate the brainstorming activity and the latter would focuse on identifying the causes or triggers of the threat scenarios. Doing so is important because different factual circumstances could give rise to failure to perform the obligatory activity or the performance of the prohibited activity. In addition, the triggers are what make the risk assessment specific to the client at hand or to the target under analysis. Therefore, all possible causes and triggers of the threat can be identified through a relevant guiding question, such as: What facts could trigger the threat at hand?

In the Section 13 example, the stakeholder meeting identifies the following triggers for the given threat scenarios: (1) Lack of documentation from third-party systems; (2) Lack of policies for updating documentation; and (3) Lack of legal knowledge. Once the triggers are identified, they can be modeled to the risk diagram as initiating threat scenarios or vulnerabilities depending on their nature. In our example, the triggers are modeled as threat scenarios (see Fig. 7).

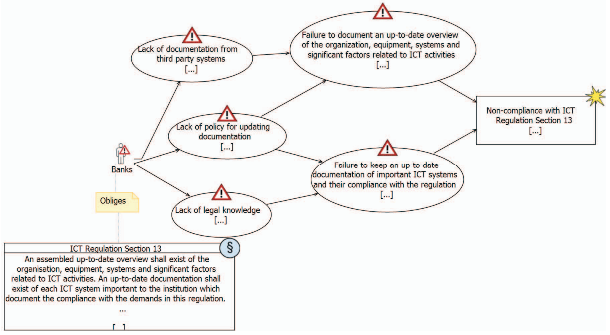
Lack of documentation from third party systems
[...]
Failure to document an up-to-date overview of the organization, equipment, systems and significant factors related to ICT activities
[...]
Lack of policy for updating documentation
[...]
Non-compliance with ICT Regulation Section 13
[...]
Banks
Failure to keep an up to date documentation of important ICT systems and their compliance with the regulation
[...]
Obliges
Lack of legal knowledge
[...]
ICT Regulation Section 13
§
An assembled up-to-date overview shall exist of the organisation, equipment, systems and significant factors related to ICT activities. An up-to-date documentation shall exist of each ICT system important to the institution which document the compliance with the demands in this regulation.
...
[...]

Fig. 7. Compliance threat diagram with triggers.

[2] This is not merely a hypothetical claim. The author has experienced a situation in which a three-hour meeting resulted in the identification of only one compliance risk. This problem stems from the lack of a structured approach for identifying compliance risks.

[3] Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT), FOR-2003-05-21-630.

In using the facts-centered approach, the template in TABLE 2 can be used to structure the facts, identify the compliance norm triggered by the facts, and schematically translate the activity in the compliance norm to threat scenarios in the same manner as in the requirement-centered approach. A difference of the facts-centered approach from the requirement-centered approach is that a certain fact could trigger the application of many compliance requirements from the same or different sources. This possibility, however, does not affect the facts-centered approach, as described here. To illustrate the facts-centered approach, let us assume that a bank is considering moving its ICT systems to the cloud. As the bank's ICT systems handle individuals' financial data, the bank is uncertain of the feasibility of adopting cloud services due to perceived compliance issues and security risks. In this context, the facts-centered approach is the most appropriate because it allows the bank to account for all possible compliance requirements which might apply to the factual circumstances at hand. In this example, the starting point for the bank is to describe the nature of cloud computing. For example, the risk analyst, with the help of cloud experts, identifies distributed server locations as inherent nature of cloud computing services. Next, compliance requirements which might be triggered by this factual situation are identified. To do so, the risk analyst could use a guiding question and ask the legal and compliance team what compliance norms such factors might trigger. Once the relevant requirements are identified, they are structured as in TABLE 2 for identifying compliance risks.

TABLE 2. TEMPLATE FOR STRUCTURING FACTS-CENTERED IDENTIFICATION

Facts	Distributed server location
Legal source	Data Protection Act Sec 29 Rundskriv 14/2010
Modality	Prohibition
Actor	Bank
Role	Data controller ICT system owner
Activity	Data Protection Act Sec 29: Personal data may not be transferred to countries which do not ensure an adequate level of protection. Rundskriv 14/2010: Banks shall not outsource their critical ICT systems to high-risk countries.
Target	Personal data ICT systems
Threat scenario	Data Protection Act Sec 29: Personal data transferred to countries which do not ensure an adequate level protection of data Rundskriv 14/2010: Outsourcing critical ICT systems to high-risk countries

TABLE 2 structures the following provisions under the Norwegian Data Protection Act[4] and Rundskriv 14/2010[5].

Sec 29: Basic conditions

Personal data may only be transferred to countries which ensure an adequate level of protection of the data.

Rundskriv 14/2010

Banks shall not outsource their critical ICT systems to high risk countries.

The artefacts in TABLE 2 can be further modeled in the CORAS approach.

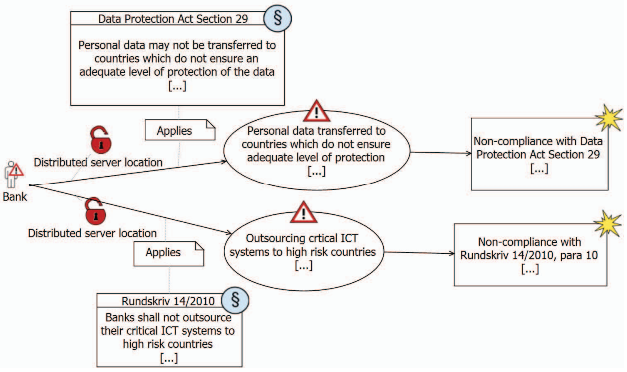
Data Protection Act Section 29
§
Personal data may not be transferred to countries which do not ensure an adequate level of protection of the data [...]
Applies
Distributed server location
Bank
Personal data transferred to countries which do not ensure adequate level of protection [...]
Non-compliance with Data Protection Act Section 29 [...]
Distributed server location
Applies
Outsourcing crtical ICT systems to high risk countries [...]
Non-compliance with Rundskriv 14/2010, para 10 [...]
Rundskriv 14/2010
§
Banks shall not outsource their critical ICT systems to high risk countries [...]

Fig. 8. Facts-centered CORAS compliance threat diagram.

As shown in Fig. 8, the risk analyst decides to model the factual circumstance as a vulnerability introduced by moving to the cloud. The meeting or brainstorming activity with the stakeholders might focus on how the distributed server location could affect the bank's compliance with these rules and on identifying the specific circumstances in which the distributed location might lead to non-compliance. The legal and compliance team identifies the following triggers: (1) The servers used to store personal data are in countries that do not ensure adequate protection; and (2) The servers are in high-risk countries. These aspects can further be modeled in the CORAS approach as threat scenarios in order to get the full picture of the compliance risks in the given context.

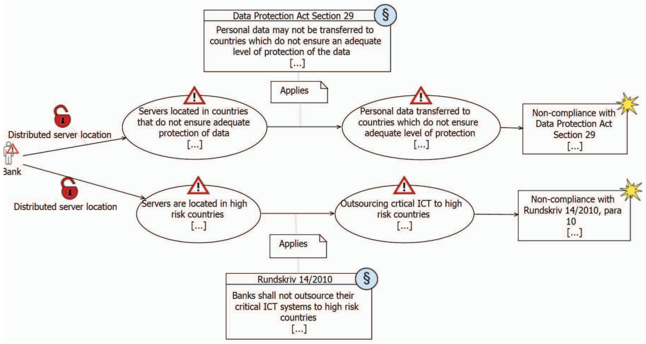
Data Protection Act Section 29
§
Personal data may not be transferred to countries which do not ensure an adequate level of protection of the data [...]
Applies
Distributed server location
Servers located in countries that do not ensure adequate protection of data [...]
Personal data transferred to countries which do not ensure adequate level of protection [...]
Non-compliance with Data Protection Act Section 29 [...]
Bank
Distributed server location
Servers are located in high risk countries [...]
Outsourcing crtical ICT to high risk countries [...]
Non-compliance with Rundskriv 14/2010, para 10 [...]
Applies
Rundskriv 14/2010
§
Banks shall not outsource their critical ICT systems to high risk countries [...]

Fig. 9. Facts-centered CORAS compliance threat model with triggers.

After completing risk identification, the risks of non-compliance should be analyzed in order to understand the

[4] Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act).

[5] Rundskriv Utflytting av bankenes IKT-oppgaver, 31-05-2010.

level of the risks, which allows the stakeholder to decide on which issues it is most important to focus. The level of the non-compliance risk is determined by considering its negative consequences and likelihood according to criteria established in advance by the stakeholders [16]. Next, the risk level (e.g., high or low risk) is established based on the consequences and likelihood of occurrence. This enables determining which non-compliance risks should be prioritized to ensure that compliance activities are directed to where they are most needed. The triggers are also prioritized. With the risks and triggers prioritized, compliance measures that can address the prioritized compliance risks are identified, and the most suitable compliance measures selected based on an assessment of their costs and benefits. Overall, this process involves analyzing the available risk control options and finally implementing the selected control mechanisms. The prioritization of risks can also be used in the monitoring and review phases, i.e., risk-based compliance checking, in order to ensure that the compliance measures address non-compliance risks in the most effective manner.

VI. Conclusion

The complexity and dynamism in the regulatory environment is increasing the need for risk-based compliance, which ensures that resources are allocated to the areas where they are most needed and compliance measures are targeted at the most significant risks. Despite the growing importance of risk-based compliance, there are few techniques for identifying compliance risks in a structured manner. This paper identifies two approaches to identifying compliance risks, the requirement-centered and facts-centered approaches. In addition, this paper proposes a technique for structuring compliance identification. This approach simplifies the identification of compliance risks by schematically translating compliance requirements into threat scenarios and unwanted incidents. This reduces the time and analytical activity involved in identifying legal and compliance risks. In future works, we will evaluate the pratical application and relevance of these approaches based on real business cases.

Acknowledgment

This work has been funded by the European Commission via the RASEN (316853) project. Thanks are also due to T. Mahler and F. Seehusen for their constant support and guidance.

References

[1] E. A. Peterson, “Compliance and ethics programs: competitive advantage through the law,” Journal of Management & Governance, vol. 17, Issue 4, Nov. 2013, pp 1027-1045, doi: 10.1007/s10997-012-9212-y.

[2] C. Giblin, A. Y. Liu, S. M¨uller1, B. Pfitzmann, and X. Zhou, “Regulations Expressed As Logical Models (REALM),” Proc. Legal Knowledge and Information Systems: The Eighteenth Annual Conference, IOS Press, 2005, pp. 37-48.

[3] Ponemon Institute, “The Role of Governance, Risk Management & Compliance in Organizations: Study of GRC practitioners,” Research Report, Sponsored by RSA, The Security Division of EMC, May 2011.

[4] R. Bonazzi, L. Hussami, and Y. Pigneur, “Compliance Manage-ment is Becoming a Major Issue in IS Design,” in A. D’Atri and D. Saccà, Eds. Information Systems: People, Organizations, Institutions, and Technologies, Springer Physica-Verlag Berlin Heidelberg , 2010, pp. 391-398.

[5] N. Racz, E. Weippl, and A. Seufert, “A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)” Proc. International Federation for Information in B. D. Decker and I. Schaumüller-Bichl, Eds.: CMS 2010, LNCS 6109, pp. 106–117.

[6] Federation of European Risk management Association, “Keys to Understanding the Diversity of Risk Management in a Riskier World”, Bench Marking Survey, 2012, 6th ed.

[7] Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Draft General Data Protection Regulation)’ Com (2012) 11 final.

[8] Article 29 Data Protection Working Party, ‘Opinion 05/2012 on Cloud Computing’ adopted on 1 July 2012 (WP 196).

[9] Opinion of the European Data Protection Supervisor on ‘the data protection reform package’ of 7 March 2012.

[10] Daniele Catteddu and Giles Hogben, Eds, “Cloud Computing: Benefits, risks and recommendations for information security” European Network and Information Security Agency, Dec. 2012.

[11] Australian Standard AS 3806-2006 Compliance Programs.

[12] COSO, ‘Enterprise Risk Management: An Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission, 2004.

[13] S.H.V. Solms, “Information Security Governance–Compliance Management vs Operational Management,” Computers & Security vol. 24, no. 6, Sep. 2005, pp.443-447.

[14] Information Commissioner’s Office (ICO), “Privacy by Design,” ICO, Nov. 2008.

[15] T. Mahler, “Legal Risk Management: Developing and Evaluating Elements of a Method for Proactive Legal Analyses, with a Particular Focus on Contracts “, University of Oslo, PhD thesis , 2010, unpublished.

[16] Australian Better Regulation Office, “Risk-based complinace,” Guide for Risk-Based Complaince Approach, Sep.2008.

[17] M.S. Lund, B. Solhaug, and K. Stølen, Model-Driven Risk Analysis: the CORAS Approach, Springer, Berlin Heidelberg, London, New York, 2011.

[18] F. Vraalsen, M.S. Lund, T. Mahler, X. Parent, K. Stølen, “Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language: Experiences and the Way Forward” in Herrmann, P. et al. (eds.): iTrust, LNCS, vol. 3477, 2005, pp. 45–60.

[19] ISO, “International Standard ISO 31000. Risk management – Principles and Guidelines on Implementation,” 2009.

[20] T. Mahler, “Defining legal risk,” Proc. Commercial Contracting for Strategic Advantage – Potentials and Prospects, Turku University of Applied Sciences, 2007, pp. 10-31.

[21] S.Y. Esayas, ‘Utilizing Security Risk Analysis and Security Testing in the Legal Domain’ in T. Bauer et al. (Eds.): ‘Risk Assessment and Risk-driven Testing’ LNCS, vol. 8418, pp. 51–67, Springer, Switzerland 2014.