Project description AGRA: Aggregated risk assessment and management

PART 1: Knowledge needs

1. Knowledge needs

Managing risk is so important that in many cases, laws and regulations impose explicit requirements on the performance, scope and frequency of risk analysis[1]. For example, this is the case for organizations that are responsible for parts of critical infrastructures, such as banking, transport, telecom, other critical ICT functions, power supply, and water supply. Non-compliance may have severe consequences for an organization, such as a costly fine or even loss of the license to operate. In a survey[2] conducted by Economist Intelligence Unit for KPMG in 2011, 55% of the respondents stated that the annual cost of GRC (Governance, Risk and Compliance) activities was between 1% and 5% of annual revenues.

Motivating example 1: A risk consultancy company has been contacted by a large bank. Before contacting the consultancy company, the bank has carried out a number of security risk analyses for different parts and aspects of their ICT systems and supporting organization, such as the central servers and physical access and damage to these, authentication mechanisms from stationary and local devices, outsourced services, availability of qualified personnel to deal with exceptional situations, and so on. The analyses have typically been initiated by managers in various units and levels of the bank organization, and each analysis has been documented in the form of written risk reports. However, this set of risk reports do not provide the overall view of the security risk picture for the whole organization that is needed by the senior management and expected by the regulatory authorities. The risk consultancy company has therefore been asked to produce a unified overall security risk report on the basis of the set of existing reports. However, they find this to be very difficult and time-consuming, as none of the standards, methods and tools available offer adequate support for such a task.

Irrespective of whether an organization has regulatory obligations with respect to risk management or not, in practice there will always be a need for risk management. Today almost all enterprises and organizations are exposed to many different kinds of risk, including security risk, operational risk, safety risk, and so on. The risk picture to which they are exposed will typically be highly complex and continuously changing. The ability to survive in a competitive market and a regulatory environment seems to be highly dependent on the ability of an enterprise or organization to deal with risk. In order to make good decisions, managers on all levels need at all times a thorough understanding of the current risk picture related to their domain of responsibility. However, obtaining such an understanding is extremely difficult and requires extensive effort and resources.

As further discussed in Section 3, a number of standards, methods, techniques and tools have been promoted to support risk management. GRC and ERM (Enterprise Risk Management)

[1] The following are a few examples from Norwegian laws and regulations: "Forskrift om IKT-systemer i banker mv" (§ 3), "Energiloven" (§ 9-3), and "Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen" (§ 2-4).

[2] The Convergence Evolution. Global survey into the integration of governance, risk and compliance. KPMG (2012).

have become major fields employing a high number of consultants and tool vendors in Norway as well as internationally.

Motivating example 2: An employee in a large company with several divisions and departments has been assigned the role of Risk Management Facilitator. One of her first tasks is to recommend a security risk management approach to be applied throughout the company. She has therefore initiated a small survey to identify the needs and preferences of the relevant actors in the organization. Based on the results, a number of requirements have been identified, including the following:

- The approach should allow managers at all levels to obtain a simple overall risk picture for their complete area of responsibility. This should be an aggregated and abstracted view of all analyses at lower levels, preferably containing no more than seven risks.
- The approach should be flexible w.r.t. specific risk analysis techniques to be used and the level of detail, as the needs and preferences vary quite a lot between departments.
- The approach should not impose strict restrictions of the assets to be addressed, as what is considered to be the important assets vary a lot between business areas, organizational units and management levels.

The Risk Management Facilitator searches available standards, methods and tools in order to find an approach on which to base her recommendation, but is unable to find any candidates that satisfy the needs and requirements of the company.

Surprisingly, the plethora of risk management approaches on offer today provides very little help for one of the major challenges of risk management, namely the following:

> *How do we ensure that the risk management approach provides each organizational unit and management level with a risk picture suitable for their particular needs while ensuring consistency between risk pictures at all times and avoiding loss of essential information?*

While a Managing Director may be concerned with big issues such as the overall information risk picture to which the organization is exposed and the potential impact of a security breach on the company reputation, a low-level technical manager may be concerned about whether opening certain ports in a firewall would imply unacceptable risk. Presenting all the risks that have been identified throughout the organization to the Managing Director at the same level of detail that is useful at the lower management levels would drown her in information that from her perspective would be next to useless. What she needs is *an aggregated and abstracted view* that summarizes the important risks for the whole organization in a comprehensible manner.

Current approaches offer little or no support for this. Composition, aggregation and abstraction are typically either not addressed at all, or based on one or more of the following techniques: 1) simply counting of the number of risks within a predefined category, 2) adding up the likelihood, consequence and/or risk level assessments for all the risks within a category, or 3) selecting only a subset of the risks identified in a detailed analyses to be escalated to a higher level, typically based on estimated risk level. Such approaches are not satisfactory, as they build on assumptions that are hardly ever fulfilled in a practical setting.

Counting the number of risks only makes sense if they are all described at the same level of detail and have approximately the same risk level. Adding up likelihood, consequence and risk assessments requires that there is no overlap or dependencies between risks, while escalating only a few selected risks means that groups of risks that may have a cumulative effect and should be considered in combination are not taken into account and that essential information may get lost. The lack of adequate support to address these issues may lead to

- costly analysis processes,
- analysis results that are not well suited as decision support for the intended user or provide only a fragmented risk picture,
- a lack of understanding of the actual risks of relevance, therefore leading to
- poor decisions.

The full risk picture for an organization will be large and complex, and therefore very hard to grasp for any human decision maker. To deal with this problem the AGRA project puts forward a new approach based on divide-and-conquer. The overall hypothesis of the AGRA project is that:

> *Providing adequate risk support to organizations requires a component-oriented approach to risk management that allows composition/decomposition and abstraction/specialization of risk models.*

By risk model we mean any representation of any risk information that is captured and documented as part of the risk management, regardless of the media or format of the documentation. Typically, a risk model may contain information about threats, vulnerabilities, unwanted incidents, likelihood estimates, consequence estimates and so on, as well as the relations between them.

PART 2: The Knowledge-building Project

2. Objectives

The main objective of the project is to develop a framework for overall unified risk management throughout an organization in order to provide a sound basis for decision making for all levels of management. The framework will have the following measurable effects:

- It will facilitate analysis and presentation of risks at different levels of abstraction depending on the role of the target group, while ensuring consistency and preservation of essential information in a common underlying risk model.
- It will be practically applicable in organizations without requiring significantly more resources in terms of effort, competence or cost than existing approaches.

Encapsulation of risk models will play a major role in the framework. By encapsulation we mean that only the elements of the risk model that are essential for the composition of risk models are externally observable. Figure 1 illustrates this concept.

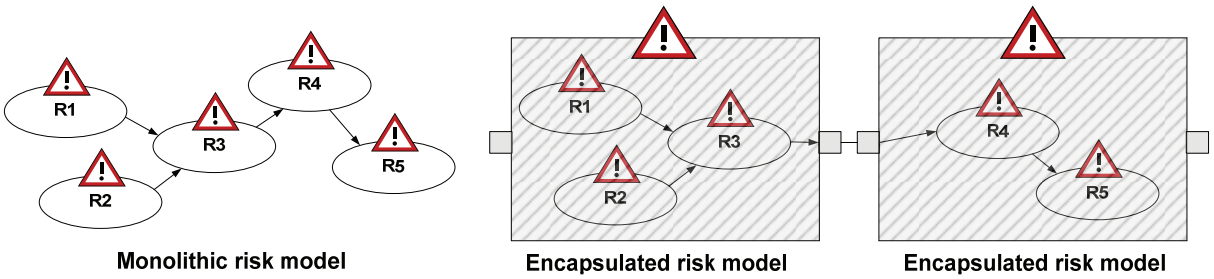

Figure 1 Encapsulation of risk models. The contents of the shaded boxes represent details that are hidden.

The left-hand part of the figure represents an approach where encapsulation is not used. A single monolithic risk model is presented with all details visible. Such approaches do not scale, and make it extremely hard to obtain an overall comprehensible risk picture as risk models grow. The right-hand part of the figure illustrates an approach where encapsulation has been exploited. Here, the monolithic model has been divided into two encapsulated risk models (represented by large shaded boxes with a warning sign on top). Each encapsulated model can be viewed and reasoned about as a single component, without worrying about its inner details. The two components have been composed via their externally observable elements (represented by the small boxes at the border of the encapsulated models). Note that although we have used a transparent grey color in the illustration to show that there is a relation between the detailed model on the left-hand side and the hidden contents of the components, it is common to use the term black box for approaches based on the hiding of details.

The AGRA framework will consist of the following parts:

- F1: A kind of black box format for risk models that captures the notion of encapsulation as described above, i.e. only the elements of the risk model that are essential for the composition of risk models are externally observable.
- F2: Support for reasoning about encapsulated risk models and their compositions. In particular, this will include composition/decomposition rules with supporting guidelines to aid practitioners.
- F3: A definition of what it means that one risk model is an abstraction of another, with accompanying guidelines for practitioners to perform abstractions aimed at a given target group, as well as to check if one risk model is a correct abstraction of another risk model.
- F4: An underlying foundation in terms of conceptual and mathematical models from which the soundness of the encapsulation principles and composition rules can be proved and a formal notion of abstraction established. In other words, this serves as the basis on which the researchers will build practical support for the end users of the framework.
- F5: Tool support for the approach aimed at practitioners. The tools will complement the guidelines and provide functionality for composition of encapsulated risk models as well as abstraction.

The successful development of each of these artefacts constitutes the sub goals of the project. Although the framework will have a wide applicability, the main focus will be on supporting risk management in the context of security.