Chapter 4
Risk Quantification Framework

In this chapter about the risk quantification framework\(^1\), first, the model – including its parameters as well as related equations and algorithms – is introduced. The model supports risk management by efficiently aggregating the individual risks for the decomposed parts of an IT scenario back to an overall risk. The second section describes simulation results regarding sensitivity analysis, identification of cost drivers, and the introduction of inaccuracy. Third, the application of the proposed risk quantification framework using a real-life business process and a prototype of a SaaS-based implementation are presented.

4.1 Model Description

The framework is build around the thought that – especially for larger IT architectures – it is hard to manage all involved risks using only a high level perspective. As the complexity of large-scale systems is too high, the model facilitates decomposition of scenarios into smaller parts, i.e., smaller scenarios for which the IT risk management process can be carried out more easily. Especially during the phases of risk identification and quantification, decision makers can, thus, better analyze and estimate potential risks. The risk quantification framework supports risk quantification by efficiently aggregating the individual risks for the decomposed parts back to an overall risk distribution.

Each scenario is assumed to consist of various components of different types. Expert interviews with IT risk management consultants showed that scenarios involving IT outsourcing are usually composed of services and data transfers. Using

\(^{1}\) Compare, in the following, Ackermann and Buxmann (2010); Ackermann et al. (2013).
visualizations such as the one shown in figure 4.1 help to better identify and quanti
ify the most critical data transfer-related risks, when data are transferred from one
service of “security zone” (e. g., an in-house service) to another “security zone”
(e. g., a service hosted by an external provider).

All of the risks, found in the conducted literature review (see section 3.1 as well
as tables A.1 and A.2) could be assigned to either services or data transfers. There
were no risks that are neither related to services nor to data transfers. Therefore,
in the following, we speak of scenarios consisting of services and data transfers.
Nonetheless, the proposed model allows incorporation of other types of scenario
components, such as people or devices.

In order to quantify risks of a given scenario and in order to calculate the risk
measure characteristics with which the scenario’s cost drivers can be analyzed, the
distribution of potential losses has to be calculated.

Our approach uses the business process with its risk parameter tables as an in-
put for the calculation. The model parameters, i. e., the variables used to describe a
scenario (e. g., a distributed business process) are described in section 4.1.1, while
two different approaches for calculating the distribution of potential losses is de-
scribed in section 4.1.2. In section 4.1.3, algorithms for deriving risk measures are
presented.

The result is presented in the form of a discrete Probability Density Function
of the Potential Losses (PDFL). See figures 4.2 and 4.15 for examples of such
functions. Based on this distribution, risk measure characteristics can be derived
using calculations provided in section 4.1.3.

4.1.1 Parameter Descriptions

In this section, all input variables of the model are successively introduced and
described. Sections 4.1.1.1 and 4.1.1.2 present the basic parameters, needed for
every scenario, while sections 4.1.1.3 to 4.1.1.5 present various possible extensions
to the base model.

4.1.1.1 Basic Scenario Parameters

In the previous section, a scenario was described to be composed of services and
data transfers. More generally, we say that a scenario consists of component types,
such as services and data transfers. The set $X$ contains all valid scenario component
types, e. g., $X = \{S; T\}$. This states that a scenario consists of two different type:
services ($S$) and data transfers ($T$). Figure 4.1 visualizes an exemplary scenario