Legal risk analysis

Kusyanti, A.

Award date:
2015

MSc Thesis

Legal Risk Analysis

A. Kusyanti

March 30, 2015

Technische Universiteit
Eindhoven
University of Technology

Printed in The Netherlands

EINDHOVEN UNIVERSITY OF TECHNOLOGY
FACULTY OF
COMPUTER SCIENCE AND ENGINEERING

The undersigned hereby certify that they have read and recommend to the Faculty of Computer Science and Engineering for acceptance a thesis entitled **"Legal Risk Analysis"** by **A. Kusyanti** in partial fulfillment of the requirements for the degree of **Master of Science**.

Dated: *March 30, 2015*

Supervisor: _____
Dr. Jerry den Hartog

Readers: _____
Dr. Nicola Zanonne

Abstract

In the healthcare service, Patients have a significant interest in protecting their personal data, as these records can have consequences for their jobs, insurance rates and other vital aspects of their lives. Data must therefore be handled by an information system that takes into account risk analysis and which must comply with the strict requirements imposed by privacy and data protection regulations. Some frameworks have already been studied with regards to risk analysis and legal analysis, such as CORAS and GR Tropos for modeling risk analysis, and Extended CORAS and NOMOS for modeling legal analysis. Based on our study, GR Tropos framework is used to model and to reason about risks within the requirements engineering process, but it cannot model laws. On the other hand, NOMOS is used to model laws, but does not consider risks in the analysis process.

In this thesis, a framework for assessing legal risk was developed by adopting the idea from GR Tropos and NOMOS. In order to perform legal risk analysis with the proposed framework, risk reasoning of GR Tropos is used and it is integrated with legal reasoning of NOMOS. The law meta-model was adopted from NOMOS while the intentional meta-model was taken from GR Tropos, which resulted in the graphical notation for modeling a scenario and capturing both the law and the intentional model. The proposed framework is developed with a-three-layer model concept by introducing the new primitive event and treatment as new constructs in NOMOS. The new constructs have been formalized so that the risk of a system could be analyzed in a legal framework. The notion of law propagation, which consists of transferable and non-transferable rights, is also presented. The proposed framework has been applied and evaluated by assessing the legal risk of a healthcare service. Based on this evaluation result, it shows that the proposed framework is able to model both the law model and the intentional model.

Acknowledgements

The final year of my MSc studies has been a special time, mixed with anxiousness and enjoyment. It would have been hard for me to reach this stage without the support of others. I would like to thank the following people, without their help and support this thesis would not have been possible.

First and foremost I would like to express my sincere thanks and appreciation to my MSc thesis tutor, Dr. Nicola Zannone. He has taught me from the scratch about Risk Analysis and Reasoning and for his daily supervision during my thesis. Once again, thank you for your patience and understanding. I will always remember it. Also Dr. Jerry den Hartog as my supervisor.

Special thanks go to Prof. Sandro Etalle as IST Coordinator in TU/e, Dr. Michel Westenberg as vice-director of the Graduate Program Computer Science at TU/e, and also Dr. E. F. Kaasschieter and Dr. Peter Veltkamp who have been helping me during my final year working on my project in Indonesia.

I would like to acknowledge International Office (STU) of TU/e, particularly Ms Mirjam Hagoort. I would also like to express my gratitude to Prof. Henk van Tilborg for the support that has been invaluable on both an academic and a personal level.

I gratefully acknowledge the funding sources that made my MSc studies possible. I was awarded a scholarship from ASML-Henkbold Scholarship. Dr. Berry Schoenmakers as my student advisor and IST Coordinator whose recommendation and support during my studies is so appreciated.

Amongst my fellow master students at Kerkoff Institute in giving such an academic environments, and to my friends in TU/e for their support and encouragement. Finally I would like to thank my parents, and my family for their constant support during the time

March 30, 2015

I studied.

Eindhoven, University of Technology A. Kusyanti
March 30, 2015

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

This thesis will discuss the subject of legal risk analysis in the healthcare system. The motivation for this thesis will be described in section 1.1. The objective of this thesis will be explained in section 1.2. The methodology of this thesis will be discussed in section 1.3, and finally the structure will be described in section 1.4.

1-1 Motivation

The latest trend with regard to patients' medical records in the healthcare industry is a move towards opportunities to change the way in which information is being recorded and distributed in the healthcare system. The healthcare industry keeps patients' medical records, develops and installs intranets in order to distribute information among associated healthcare providers, and also uses the internet to share information relating to healthcare. Information sharing between different healthcare organizations is critical for efficient and cost-effective healthcare service delivery.

Medical records include information that is extremely sensitive in nature. The security and privacy of patients' information are concerns shared by all healthcare organizations. In the healthcare environment, even an insignificant loss of information may prove to be a serious turn of events with regard to the security of a system. A typical threat to a healthcare information system is an unauthorized person gaining access to patients' medical records. As a consequence, an electronic healthcare system must be considered as a new risk scenario with regard to the protection of patients' sensitive personal data.

Patients have a significant interest in protecting their personal data, as these records can have consequences for their jobs, insurance rates and other vital aspects of their lives. Data must therefore be handled by an information system that takes into account risk analysis

and which must comply with the strict requirements imposed by privacy and data protection regulations. However, privacy and data protection regulations are expressed in terms of a set of legal concepts, such as rights, obligations and privileges, while requirements are expressed in terms of stakeholder goals. As privacy and data protection regulations and requirements are expressed in different terms, the law needs to be modeled and analyzed with the purpose of establishing compliance with a set of system requirements. The problems associated with modeling and analyzing the law with the purpose of establishing the compliance of an Information Technology (IT) system with legal requirements in risk analysis within some frameworks will be studied in this thesis.

Some frameworks have already been proposed, such as CORAS [1] and GR Tropos [2] for modeling risk analysis and Extended CORAS [3] and NOMOS [4] for modeling legal analysis. The GR Tropos framework models and reasons about risks , but it cannot model laws. On the other hand, the NOMOS framework was developed in order to model law without considering risks in the analysis process. Therefore, in this thesis, a new framework for assessing legal risk is proposed by integrating GR Tropos and NOMOS. The new framework is based on a meta-model which takes risks into account, and uses graphical notations to capture both the law model and the goal model. In this work, the concept of law propagation will also be introduced. The proposed approach will be implemented within the IT system which deals with hospital medical records. In this thesis, it will be used to evaluate the compliance of a hospital IT system with the European Data Protection Directive.

1-2 Thesis Objective

The problem of modeling and analyzing law for the purpose of establishing compliance with a set of system requirements in the process of risk analysis will be studied in this thesis. The final objectives of this thesis are:

1. To present experiences of using CORAS, GR Tropos and NOMOS to specify legal risk scenarios.
2. To present ideas regarding the integration of GR Tropos and NOMOS, which will result in a conceptual model in which legal aspects are integrated within the risk analysis process.

1-3 Methodology

To achieve these objectives, the methodology that will be used in this thesis is conducting systematic studies. Conducting studies in several frameworks (CORAS, GR Tropos and NOMOS) will provide us with various facts. Based on these facts, a new framework will be proposed.

1-4 Organization of the Thesis

The thesis will be organized as follows.

- **Chapter 1 Introduction**. This chapter provides an introduction to the research domain, as well as the objectives and organization of the thesis.
- **Chapter 2 Scenario**. This chapter introduces the Personal Health Record (PHR) system, the legal aspects of the healthcare system and a typical scenario in the healthcare domain.
- **Chapter 3 Related Works**. This chapter introduces the state-of-the-art of risk analysis and legal analysis.
- **Chapter 4 Legal Risk Analysis Frameworks**. This chapter contains a discussion of the existing legal risk analysis frameworks and the findings from the studies.
- **Chapter 5 Proposed Framework**. This chapter presents the proposed framework based on the integration of the GR Tropos and NOMOS frameworks in order to support legal risk analysis.
- **Chapter 6 Evaluation**. This chapter presents the application and evaluation of the proposed framework within a healthcare scenario.
- **Chapter 7 Conclusion**. This final chapter discusses the conclusion and contributions of this thesis, and also presents the future work.

Chapter 2

Use Case

This chapter introduces a typical scenario in the healthcare domain. The scenario will be used to discuss the main legal issues in the field of healthcare. Section 2.1 will provide an introduction to the Personal Health Record (PHR) system. The complete scenario involving the healthcare systems that have implemented PHR will be discussed in section 2.2. In section 2.3, the legal aspects of the healthcare system with regard to data protection regulations are described. Finally, the legal issues involved in the healthcare system scenario are presented in section 2.4.

2-1 PHR (Personal Health Record) System

Customarily, medical treatment documentation that needs to be accessible to healthcare professionals is stored in a paper-based system. Paper-based medical records have several weaknesses, such as illegible handwriting, poor availability and data which have not been updated. As paper records still represent the most commonly used medium for obtaining and storing patients' medical records, they could inhibit the continuity and quality of the care which patients receive.

The implementation of PHR systems constitutes an important advancement in the quality of patient care, as these systems can enhance readability, availability and data quality. PHR is a patient-directed information tool that enables patients to store and collect information from different sources regarding the past and present state of health of an individual over a considerable period of time [5]. The concept behind PHR is the need to compile medical records and the associated documents and to enable patients to access and manage their medical information and to share it with those who need it. PHR data are accessible in electronic form to all authorized healthcare professionals and other

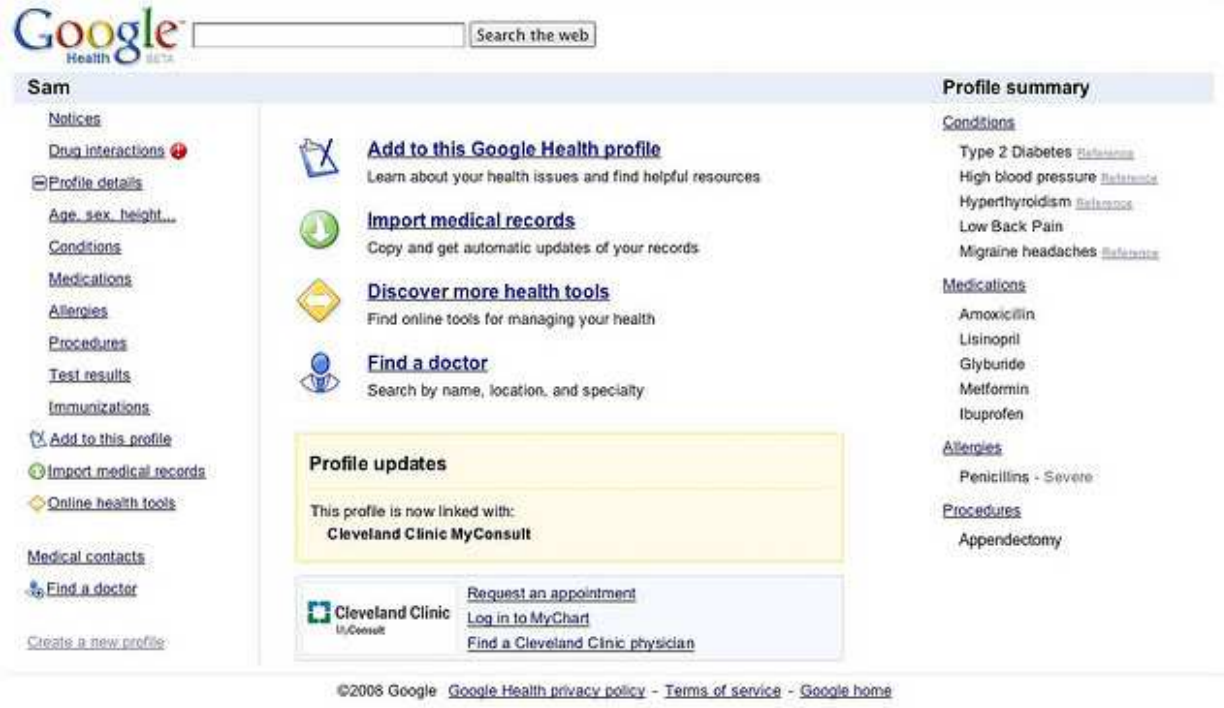

Figure 2-1: Google Health

authorized institutions wherever and whenever the data are needed, and ensure greater quality and security with regard to medical information than the traditional forms of medical documentation.

One of the examples of PHR is Google Health [6], which allows patients to manage their own medical data regarding their current and previous medications, allergies, procedures, immunizations, conditions and test results from various sources of healthcare information. Google Health has several features: it organizes online health profiles and transfers and shares medical records between hospitals and any other health-related organizations. It is beneficial in that it allows patients to manage their own healthcare, improve communications with their doctors and ensure that more complete and correct information is provided to healthcare providers than the current paper-based system. Another service that has similar functions is Microsoft HealthVault [7]. The difference between Google and Microsoft in this case is that Google focuses on the consumer while Microsoft has used its Amalga technology in order to help hospitals to organize their electronic data. Figure 2-1 and Figure 2-2 depict screen shots of Google Health and Microsoft HealthVault respectively.

From the point of view of data protection, the fact has to be stressed that PHR systems have the potential not only to process more personal data, but also to make a patient's data more readily available to a wider circle of recipients than ever before. Maintaining health records

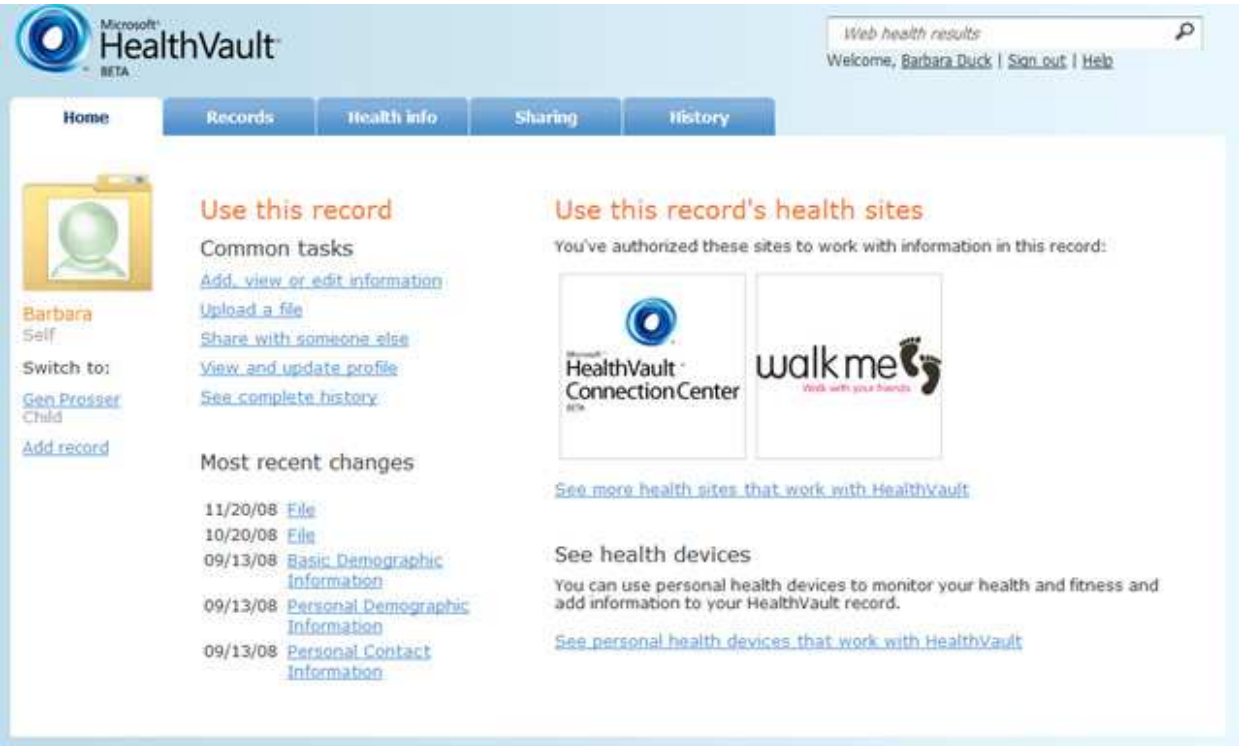

Figure 2-2: Microsoft HealthVault

in an electronic form increases the risk that patients' information could be accidentally exposed or easily distributed to unauthorized parties. The release of identifiable individual information can happen intentionally or inadvertently; it can occur within an organization or be the result of an external breach of security. As an example, a few weeks after a woman from Orlando had been to her doctor for some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol, as reported in Orlando Sentinel. Another example as reported by The Ann Arbor News is that of a Michigan-based health system which accidentally posted the medical records of thousands of patients on the Internet [8]. Regardless of how or why a person's health privacy is disclosed, the effect on the individual is the same.

2-2 Scenario Description

In this section a healthcare scenario featuring a PHR system is presented. The scenario is depicted in Figure 2.3. The focus in this scenario is on Alice, a 30-year-old woman who is the patient. The scenario consists of several actors:

- **The Patient**
  who has information regarding his or her health and needs medical treatment and

services;

- **A PHR Provider**
  who manages the patients' information.
- **The Hospital**
  that acts as health care treatment provider.
- **The Laboratory (Lab)**
  which carries out medical tests and examinations for the hospital.
- **The Researcher**
  as an actor who carries out research for medical studies.
- **The Insurance Company**
  which manages the patients' insurance.
- **The Ethical Committee**
  which monitors the researcher's actions.
- **The Privacy Authority**
  which is responsible for monitoring the hospital.

Figure 2-3 shows the complete scenario. In this scenario, Alice chooses a PHR Provider and shares her information with a PHR provider that is chosen by her. Basically, the PHR Provider needs to collect information from the patient in order to provide the hospital and the insurance company with the information required for certain services, which are medical treatment and insurance assistance. The patient's information is comprised of two parts, which are medical records and personal information. Medical records contain information that is related to the patient's health and condition, medication, allergies, procedures, immunizations and test results, while personal information is information that contains the patient's identity, such as his or her name, address and contact details. The PHR provider will share medical records with the hospital for the purpose of medical treatment, while personal information will be shared with the insurance company in order to obtain insurance assistance.

In this case, when Alice is involved in an accident, she needs medical treatment and insurance assistance provided by the hospital and the insurance company, respectively. Based on the consent given by Alice, the PHR provider will disclose her personal information to the insurance company in order to obtain insurance assistance. The PHR provider will also disclose Alice's medical records to the hospital so that she can access medical treatment. With regard to medical treatment, if necessary, the hospital may need some medical tests to be carried out by other laboratories. The hospital then will disclose Alice's medical record to the laboratory with her consent.

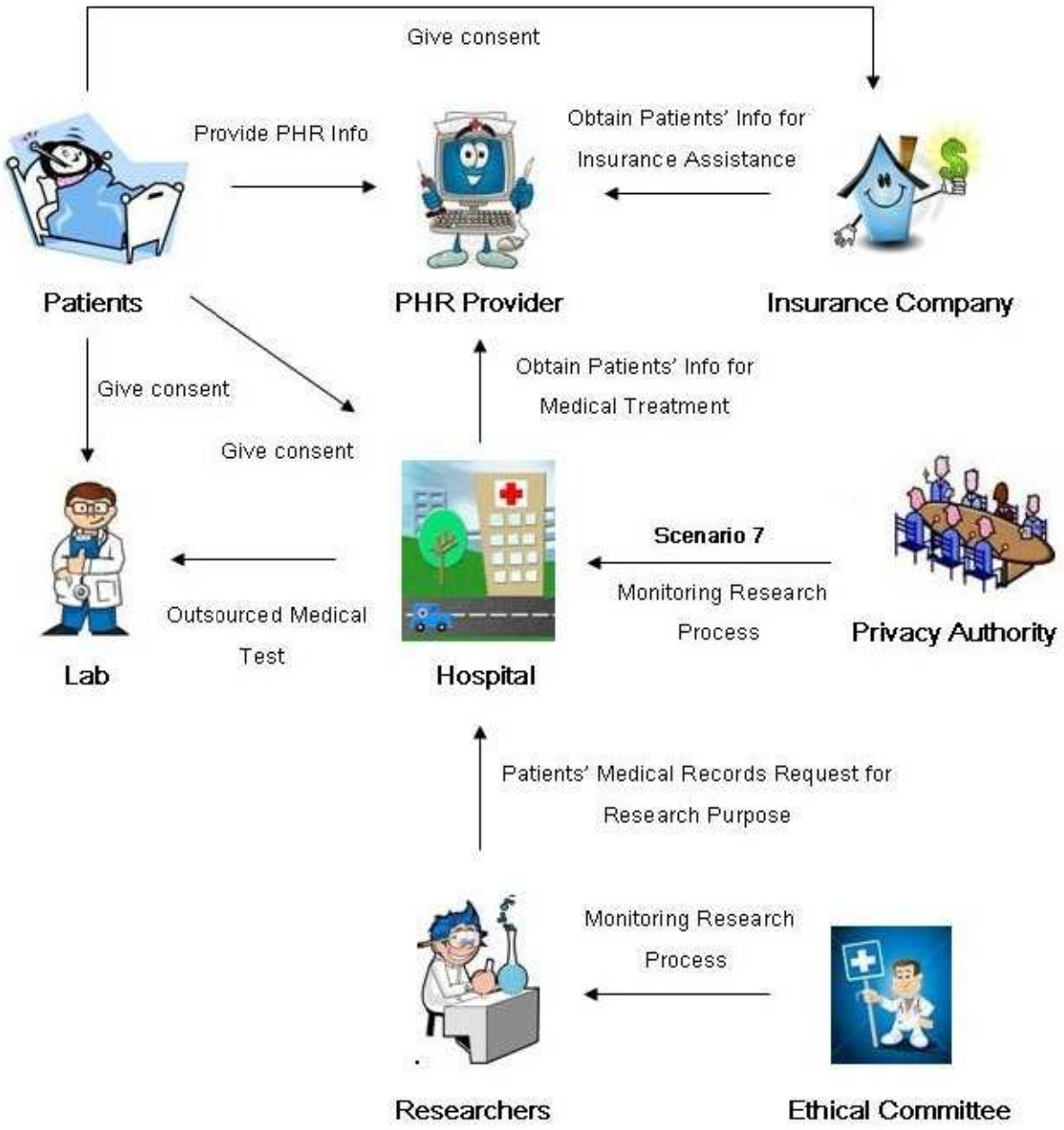

Figure 2-3: PHR Scenario

If Alice is suffering from an epidemic disease, such as cholera, then the researchers will collect her medical information for research purposes. Researchers are responsible for preventing, screening and surveying epidemics and for gaining each patient's medical record from the hospital for research purposes, including Alice's medical information.

This scenario can be divided into seven sub-scenarios as shown below, which will be discussed in more detail in section 2.4.

- **Scenario 1**
  Alice chooses a certain PHR Provider to manage her personal health information;
- **Scenario 2**
  Alice requests the assistance of the PHR Provider in obtaining insurance assistance from the Insurance Company;
- **Scenario 3**
  Alice requests the assistance of the PHR Provider in obtaining medical treatment from the Hospital;
- **Scenario 4**
  The Hospital needs the Lab to perform medical tests;
- **Scenario 5**
  The Researchers need to collect the Patient's medical record for their research from the Hospital;
- **Scenario 6**
  The Ethical Committee monitors the Researchers with regard to their medical research;
- **Scenario 7**
  The Privacy Authority monitors the Hospital with regard to the protection of the Patient's data and privacy compliance.

2-3 Data Protection Regulation

Within the European Union (EU), data protection has become the most highly-regulated worldwide jurisdiction. The fundamental right to the protection of personal data is essentially based on the EC Data Protection Directive 95/46/EC [9] regarding privacy and electronic communications. The Directive provides guidelines for the collection, use, storage, distribution and other forms of processing of personal data in the Member States.

Personal data processing, which includes providing personal data, must comply with the Directive. Personal data are explained as being any information relating to an identified or

identifiable natural person or data subject, as mentioned in Article 2(a), including sound and image data relating to natural persons. According to the Directive, an identifiable person is a person who can be identified directly or indirectly from the data in conjunction with other factors.

All personal data in medical documentation and in PHR systems are considered to be sensitive personal data. Therefore, they are not only subject to the general rules regarding the protection of personal data in the Directive, but also to the special data protection rules on the processing of sensitive information.

The Directive 95/46/EC on the protection of personal data has several articles which define various subjects whose rights and obligations are regulated in relation to the processing of personal data:

Data Subject is the person to whom the personal data relate. The data subject is granted several rights, namely the Right to Information (Article 10), the Right of Access (Article 12) and the Right of Object (Article 14). Once the personal data are provided by the data subject, the data subject is granted the right to be informed of the identity of the data controller and of the purposes of the data processing, as stated in Article 10. Based on Article 12, the data subject is granted the right to access. In cases in which personal data do not comply with the Directive due to inaccuracy or incompleteness, then the rectification, erasure or blocking of data can be conducted. Furthermore, if his or her personal data are disclosed for the purpose of direct marketing without any notification being given, then the data subject is granted the right to object, as stated in Article 14.

Data Controller as defined in Article 2 shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. As stated in Article 6, due to principles relating to data quality, during data collection, data controllers must inform the data subject of the purposes for which the data are being collected. In processing these personal data, data controllers must process the personal data fairly and lawfully. Personal data should be accurate, up-to-date, adequate, relevant and not excessive. Moreover, these data should be kept for longer than is necessary for the purposes for which the data were collected or for which they are being processed for historical, statistical or scientific purposes. Article 17 of the Directive imposes an obligation upon data controllers to implement appropriate technical and organizational measures to protect personal data against accidental or illegal destruction, accidental loss, alteration, unauthorized access or communication or any other form of processing. These measures shall ensure an appropriate level of security.

Data Processor as defined in Article 2 shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller. Processing personal data includes anything that can be done with the personal data automatically or manually. As stated in Article 7 with regard to the criteria for legit-

imizing data processing, basically, personal data can be processed only if the data subject has unambiguously given his/her consent. Moreover, personal data can be processed for the purpose of complying with a legal obligation or in order to protect the vital interests of the data subject or in order to make the data accessible to the public. The processing of special categories of data is explained in Article 8. This article states that personal data can be processed for the purposes of preventive medicine, medical diagnosis and the provision of care or treatment. Moreover, the data could be processed without the data subject's consent if the data subject is physically or legally incapable of giving his/her consent, with an intervention from the authorization of his/her representative or an authority or a person provided by the law. In addition, personal data can be processed for historical, statistical or scientific purposes, as stated in Article 6.

Based on Directive 95/46/EC of the European Parliament and of the Council on the Protection of Personal Data, it is not only the Data Subject, the Data Controller and the Data Processor who play a role, but also the Ethical Committee and the Privacy Authority.

Ethical Committee. The necessity of an ethics committee in medical research is also stated in the Directives. The ethics committee's role as an assistant to the Commission in taking community measurements is regulated in Articles 31 and 17, in which ethics committees are obliged to implement appropriate technical and organizational measures in order to protect personal data against accidental or illegal destruction, accidental loss, unauthorized access, alteration, communication or any other form of processing in order to ensure the confidentiality, integrity and accuracy of the processed data.

Ethics committees for research have a significant role to perform in ensuring the ethical standards and scientific merit of research which engages with human subjects. The obligations of ethics committee are mainly divided into three parts:

- **Obligation to research participants**
  The ethics committee has to ensure that the rights of the research participants are protected, and to ensure that they receive sufficient information regarding the research;
- **Obligation to society**
  Research ethics committees have an obligation to society as it provides the resources for research to be conducted, and because society will be affected by the research findings;
- **Obligation to the researcher**
  The obligation of an ethics committee to the researcher is to treat the research proposal with respect and consideration.

Privacy Authority. Article 28 of the Directive mentions that privacy authorities have certain powers, such as consultative powers, investigative powers, effective powers

of intervention, the power to engage in legal proceedings or to bring violations to the attention of judicial authorities, and the power to deal with complaints.

In general, based on the Articles discussed above, the principles of data protection regulation in health care systems are:

- **Limitation Principle**
  The limitation principle is outlined in Article 6(1)(b) of the Directive which prohibits further processing that is irrelevant to the purposes of the data collection;
- **Data Quality Principle**
  The data quality principle as outlined in the Directive states that personal data must be relevant and must not exceed the purposes for which they are collected. In addition, the data must be accurate and kept up-to-date. Hence, any data that are not relevant must not be collected, and in cases in which they have been collected, they have to be discarded (Article 6(1)(c));
- **Retention Principle**
  The retention principle states that personal data must be kept for no longer than is necessary for the purpose for which the data were collected or further processed ;
- **Information Requirements**
  According to Article 10 of the Directive, in processing PHR information, the Data Controller has to give certain information to the Data Subjects, such as information on the identity of the controller and the purposes of the processing;
- **Data subject's right of access**
  Article 12 of the Directive states that data subjects are provided with the ability to check the accuracy of the data and to ensure that the data are kept up-to-date.

2-4 Legal Issues in the Scenario

This section presents a legal requirement analysis of the scenario given in section 2.2 with regard to the EU Data Protection Directive. Any treatment of medical data that are categorized as sensitive data will have to adhere to the basic principles of data protection. Therefore, any processing of personal data in PHR systems must fully comply with the rules for the protection of personal data.

Based on the Directive, in our scenario the Patient plays the role of the data subject, while the PHR Provider acts as a data controller. Any legal subject that acts on behalf of the PHR Provider is a data processor, such as a Researcher, the Laboratory, the Hospital, and the Insurance Company.

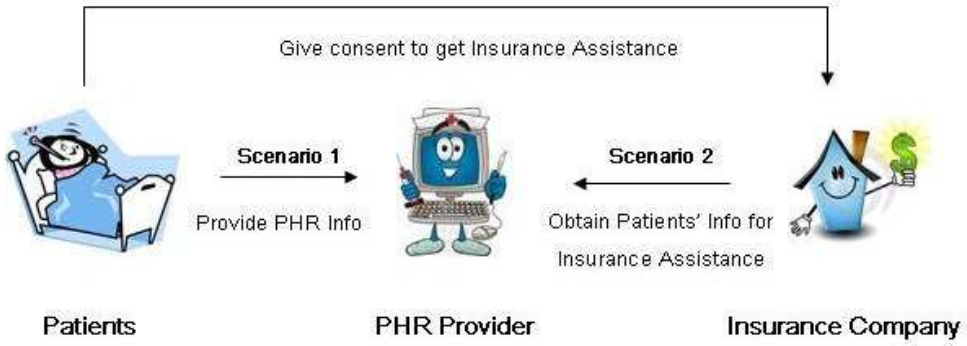

Figure 2-4: Scenario 1 and Scenario 2 of PHR System

In Scenario 1, Alice chooses a certain PHR Provider to manage her personal health information. In order to help Alice to obtain medical services and insurance assistance, the PHR Provider has to obtain her personal health information. In principle, these personal health information data should be collected and processed only by healthcare professionals or individuals or bodies working on behalf of healthcare professionals, which means that the PHR Provider is allowed to collect and process medical data. During the process of obtaining the patient's information, the data should not be inadequate, irrelevant and excessive, as mentioned in Article 6(1)(c). The patient's information is comprised of two parts, which are medical records and personal information. Moreover, in this case, once the PHR Provider has the patient's information, the Patient must be granted the right to be informed, as outlined in Article 10. Moreover, the Patient must be granted the right to access, and if the patient's information is not correct, the data can be rectified, erased or blocked, as stated in Article 12. The PHR Provider is not allowed to give Alice's medical data to any third parties for business purposes; otherwise, Alice can use the right to object, as outlined in Article 14. Figure 2-4 depicts Scenario 1 and Scenario 2 of the PHR System.

In Scenario 2, Alice requests the assistance of the PHR Provider in obtaining insurance assistance from the Insurance Company. The PHR Provider will disclose PHR Information with the consent of the Patient to the Insurance Company that is strictly necessary for the company to carry out its work. The PHR Provider cannot disclose this PHR information without the patient's consent, as stated in Article 7. In this case, the Insurance Company should not have an access to Alice's medical records, but should only be informed of her personal identity data and her insurance policy number. The disclosure of the patient's data to the Insurance Company should be relevant to the extent to which the data are used, as described in Article 6(1)(b), as the Insurance Company should inform the purposes of the processing for which the data are intended.

In Scenario 3, it is similar to Scenario 2, Alice requests the assistance of the PHR Provider in obtaining medical treatment from the Hospital. The Hospital needs the patient's medical data, which it obtains from the PHR Provider. The PHR Provider discloses this information with the consent of the Patient. The PHR Provider cannot disclose this PHR Information without the consent of the Patient, as stated in Article 7. In cases in which the Patient is physically incapable of giving his/her consent, an intervention may only be carried out on a person who does not have the capacity to consent, as explained in Article 8. Information about the state of health or other personal circumstances of an individual within the field of healthcare must not be disclosed unless it is clear that its disclosure will not constitute any harm to the person concerned. The disclosure of a patient's data to the Hospital should be relevant to the extent to which the data are going to be used, as described in Article 6.

In Scenario 4, the Hospital needs a Lab to carry out a medical test. As the Hospital outsources its medical tests to a partner lab, when the Hospital needs a medical test for the Patient, the Lab needs Alice's medical data. The Hospital has to disclose this information in order to get the task done by the Lab with Alice's consent. The Hospital cannot disclose this PHR Information without the consent of the Patient, as stated in Article 7. However, in cases in which the Patient is unable to consent, an intervention may only be carried out by a person who does not have the capacity to consent, as explained in Article 8. The disclosure of Alice's data to the Lab should be relevant to the purposes of the medical tests, as described in Article 6. Figure 2-5 depicts Scenario 3 and Scenario 4 of the PHR System.

In Scenario 5, the Researchers need to collect the patient's medical record from the Hospital for their research. Researchers play the role of data processors, as they are responsible for conducting research with patients' medical data, and thus they can access patients' personal data. The patient's data can be given to the Researchers for further data processing for historical, statistical or scientific reasons, as stated in Article 6. In this case, beforehand the Patient has already given her consent for the collection of her medical records, as mentioned in Article 7. Once again, the Patient has already been informed about why this information is being collected, as described in Article 10 (the right to be informed). Figure 2-6 depicts Scenario 5, Scenario 6 and Scenario 7 of the PHR System.

In Scenario 6, the Ethics Committee monitors the research process. The independence of this Ethics Committee is guaranteed by law, and the Ethics Committee should be a multidisciplinary team consisting of specialist doctors, general practitioners, pharmacists, nurses, psychologists, an ethicist, a social scientist and a person who is qualified in legal matters, and also representatives of the Patients. In the case of medical research, laws covering data collection procedures have adversely affected the work of the Researchers.

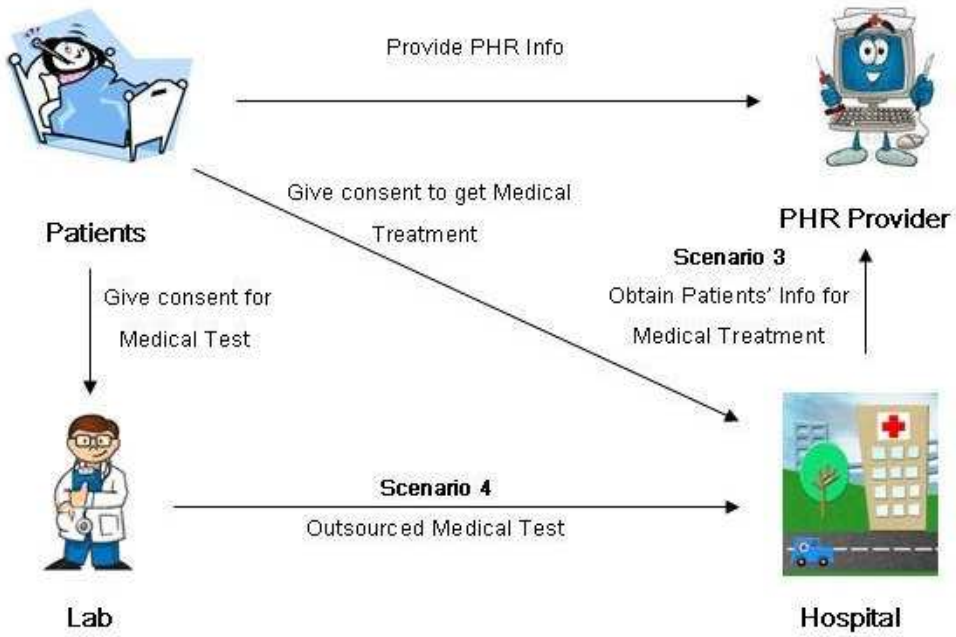

Figure 2-5: Scenario 3 and Scenario 4 of PHR System

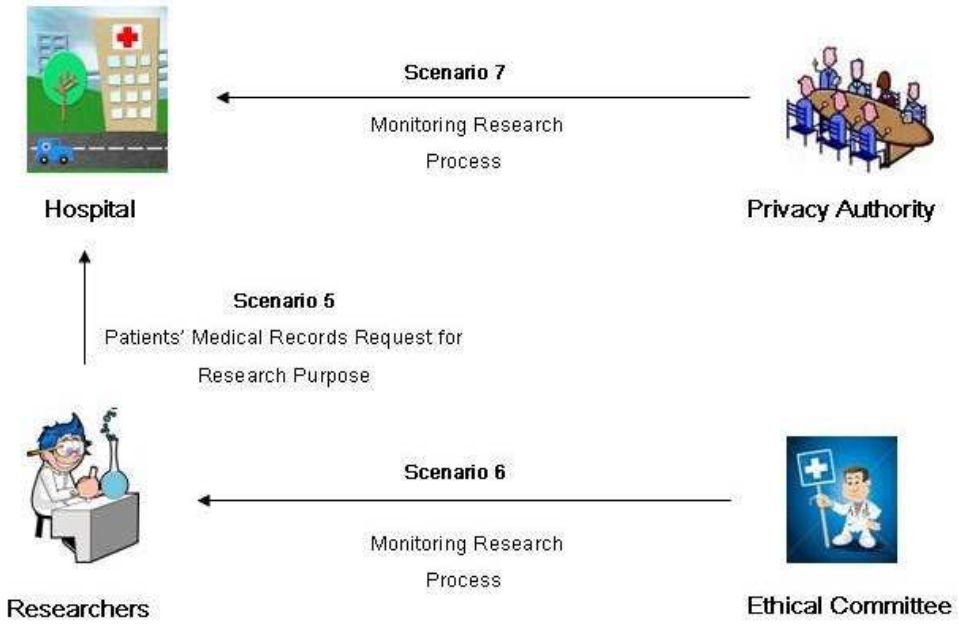

Figure 2-6: Scenario 5, Scenario 6, and Scenario 7 of PHR System

This research is expected to meet the public's need for knowledge and to provide information that will help both individuals and the community. This research process will be monitored by the Ethics Committee, as stated in Article 31.

Scenario 7, the final scenario, arises because of the need for an independent working party, which is called a Privacy Authority for the protection of personal data. In the research process outlined in Scenario 5, the Researchers collect the patient's medical record from the Hospital for their research. The Hospital, as the data center during this research process, must be monitored. The Privacy Authority is responsible for this monitoring and for the protection of personal data, as mentioned in Article 28.

Chapter 3

Related Works

In this chapter, all of the related works that deal with the risk management process and legal analysis will be discussed. Risk management will be explained in section 3.1, while legal analysis will be discussed in section 3.2.

3-1 Risk Management

The ISO/IEC Guide 73 [10] defines risk as the combination of the probability of an event and its consequences, whereas risk management encompasses the policies, procedures and practices involved in the identification, analysis, assessment, control, avoidance, minimization and elimination of unacceptable risks.

Detailed explanations of the risk management process and methods will be discussed in the remainder of this section.

3-1-1 Risk Management Process

The risk management process is a systematic application of activities undertaken by an organization in order to control and minimize threats to the continuing efficiency, profitability and success of its operations [10]. Risk itself is defined as the combination of the probability of an event and its consequences by the ISO/IEC Guide 73. The entire risk management process is depicted schematically in Figure 3-1, which will be explained in more detail later on.

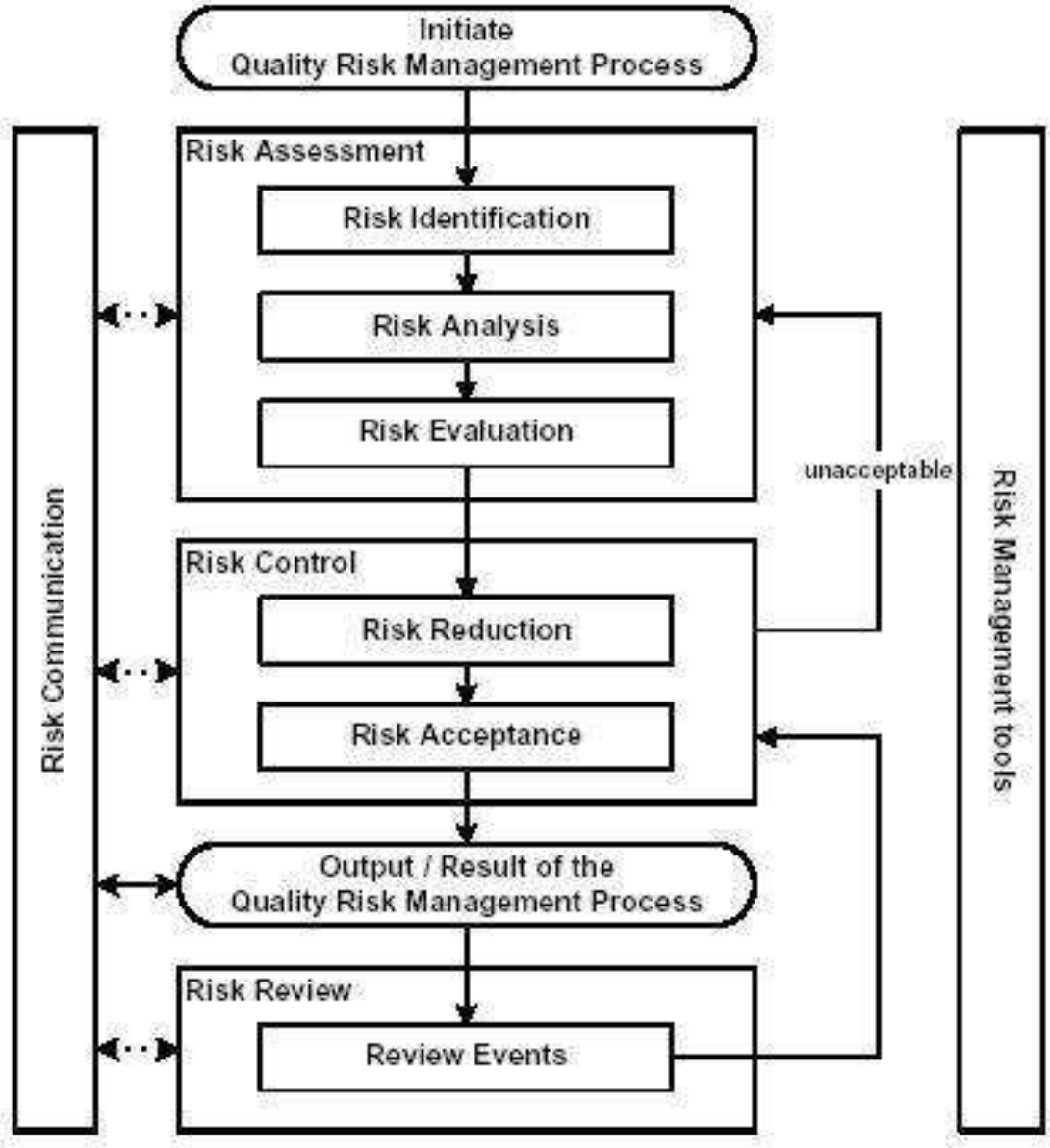

Figure 3-1: Risk Management Process

Risk Assessment

Risk Assessment is defined by the ISO/ IEC Guide 73 as the overall process of risk identification, risk analysis and risk evaluation.

1. **Risk Identification**
   Risk Identification is the process of finding, recognizing and describing risks in an organized way in order to assure that all of the important activities in the organization have been identified and categorized. This needs a detailed knowledge of the organization and the legal, social, political and cultural environment in which it exists, including the threats and opportunities relating to the achievement of its objectives. By taking into account the consequences and probability of risks, it is possible to prioritize the key risks that need to be analyzed in more detail.

2. **Risk Analysis**
   Risk Analysis is the process of determining the level of risk, identifying the probability and impact of risks and classifying similar or related risks. There are two types of risk analysis: quantitative and qualitative risk analysis. Quantitative risk analysis uses numerical values that may be derived from experimental data, by the extrapolation of experimental studies on related systems or from historical data, while qualitative risk analysis uses relative descriptions of likelihood and adverse outcomes and combines data derived from several sources, some of which may be quantitative. The use of the qualitative or quantitative approach depends on the amount, type and quality of the data, the complexity of the risk under consideration, and the level of detail required for decision-making [10].

3. **Risk Evaluation**
   After the risk analysis process has been accomplished, it is necessary to compare and evaluate the estimated risks against established risk criteria in order to determine whether or not the level of risk is acceptable or tolerable. Risk evaluation is a process that focuses on assessing the probability and impact of risks.

Risk Control

Risk Control is an action which is intended to monitor, reevaluate and check the degree of compliance with risk management decisions [10].

1. **Risk Reduction**
   Risk Reduction is the process of reducing the probability or negative consequences (or both) associated with a risk. Outsourcing is an example of risk reduction. Outsourcing is performed when the outsourcer demonstrates a higher capability with regard to managing or reducing risks.

2. **Risk Acceptance**
   Risk Acceptance is the decision to accept a certain degree of risk for technical or cost-related reasons.

Risk Review

A Risk Review consists of an overall assessment of the status of risks in a project, monitoring the progress of risk reduction actions and ensuring the continued application of the risk.

1. **Review Events**
   Review Events is an activity designed to decide the suitability, efficiency and effectiveness of the subject matter in order to achieve established objectives.

During the entire risk management process, there is an interactive process of information and opinion exchange among the interested parties. This activity is called risk communication and involves multiple messages about the nature of risks or expressing concerns, opinions or reactions to risk messages.

3-1-2 FMEA/ FMECA

Failure Mode Effect Analysis/Failure Mode Effect and Criticality Analysis (FMEA/FMECA) [11] is a technique that is used to assess the potential failures of individual components within a system. FMEA/FMECA proposes qualitative values (i.e., frequent, reasonably probable, occasional, remote and extremely unlikely). In FMEA/FMECA, events are prioritized using the notion of loss expectancy, which is defined on the basis of the likelihood of events and their severity. This priority represents the criticality of an event. When resources are limited, analysts can decide to adopt countermeasures in order to mitigate events on the basis of their priority.

These are the basic steps of the FMEA/FMECA procedure:

1. Identify the functions, failures, effects, causes and controls for each process to be analyzed;
2. Evaluate the identified risk;
3. Prioritize and assign corrective actions;
4. Perform corrective actions and re-evaluate risk;
5. Distribute and review the analysis.

With regard to the risk management process described in the previous section, these five basic steps of FMEA/FMECA are covered in the risk assessment process. Risk communications in FMEA/FMECA are performed by assembling a team and establishing basic rules for the item to be analyzed. The first step encompasses the risk identification process along with the risk analysis process. The second equates to the risk evaluation process, while the third and fourth processes are considered to translate as risk control. The final step can be considered to be a risk review process, even though FMEA/FMECA also has its own risk evaluation methods, which are risk priority numbers and criticality analysis. The results are then documented in a table in which each separate module's potential failure modes are investigated with regard to the relevant failure detection method, failure effect and criticality.

3-1-3 HazOp

Hazard and Operability (HazOp) analysis [12] is a risk identification method that is used to identify and evaluate potential hazards and operability problems. The objective of HazOp is to discover system behaviors which may deviate from the intended design, and to determine whether or not these deviations may cause unwanted incidents (hazards). During examination sessions, HazOp attempts to visualize all possible deviations from every design and operating intention. In HazOp, guidewords are used to mitigate weaknesses, and they are used to guide and to stimulate creative thinking towards appropriate deviations. Table 3-1 shows the list of guidewords used in HazOp. The HazOp process can be seen in more detail in Figure 3-2.

The way in which guidewords are used depends on the system that is being analyzed. In the case of a product distillation unit at a refinery company, the guidewords *"High Pressure"* will mean water with a high pressure is flowing inside the pipe or in the condenser [13].

A similar technique called Hazard Identification (HazId) is used in safety analysis. HazId is an analysis process for smaller risks, which is basically a simplified version of HazOp. HazId uses checklists instead of guidewords, and is often used in the early stages of the analysis process. The results of HazOp are also presented in a table, like the FMEA/FMECA tables.

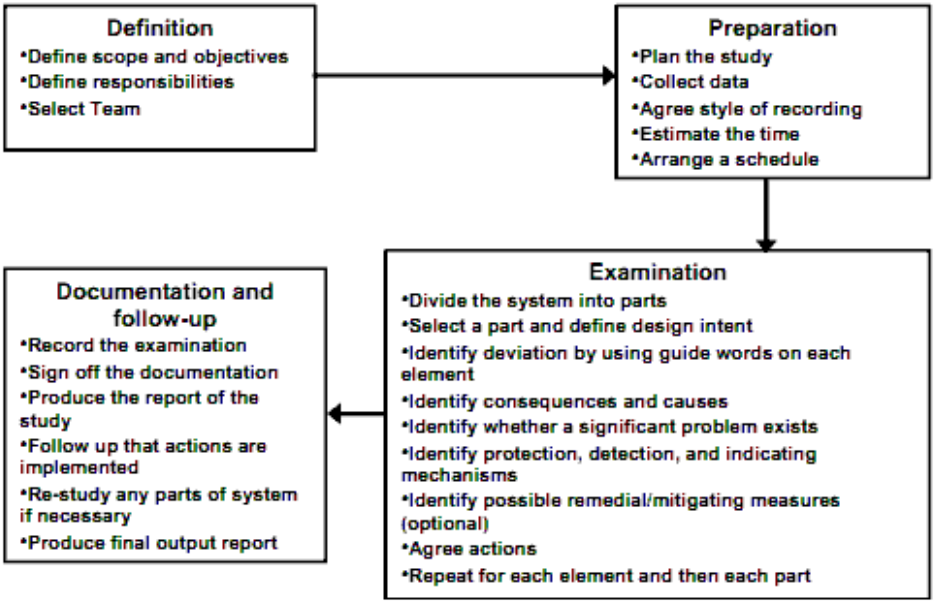

Figure 3-2: Hazop Process

Table 3-1: Guided-word and Meaning

Guided-word	Meaning
No (Not, none)	None of the design intent is achieved
More (More of, higher)	Quantitative increase in a parameter
Less (less of, lower)	Quantitative decrease in a parameter
As well as (more than)	An additional activity occurs
Part of	Only some of the design intention is achieved
Reverse	Logical opposite of the design intention occurs
Other than (other)	Complete substitution - another activity takes place

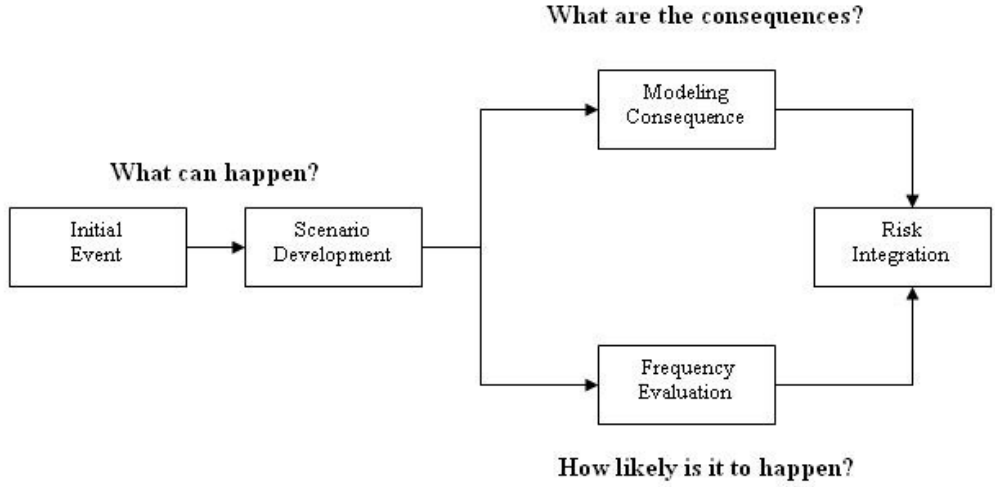

Figure 3-3: Probabilistic Risk Analysis Process

In principle, all of the steps taken in HazOp or HazId are covered in the risk management process described in the previous section, starting from risk identification using guidewords (in HazOp) or a checklist (in HazIp), and ending with the risk review, which uses tables to present the results.

3-1-4 Probabilistic Risk Analysis

Probabilistic Risk Analysis (PRA) [14] is a method of validating claims of safety. PRA is used to demonstrate the need for further improvement. In PRA, risk is defined by two quantities, namely the magnitude (severity) of the possible adverse consequences of the event and the probability of the occurrence of each consequence. As a quantitative approach, PRA assigns probability values to each potential consequence of alternative decisions, and then summarizes the overall value of each alternative decision using the expected value of its consequences. Basically, PRA answers three basic questions:

1. What can happen?
2. How likely is it to happen?
3. If it happens, what are the consequences?

The implementation of the threefold definition of risk in PRA can be seen in Figure 3-3. The process starts with an initiating event that alters the system and causes a scenario to

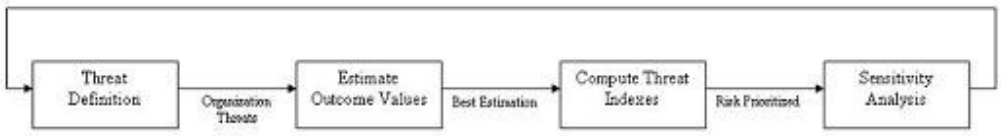

Figure 3-4: Multi Attribute Risk Assessment

develop. The scenario is developed in order to assess the risk analysis process. During the development of the scenario, there are also additional failures that may lead to undesirable consequences. Afterwards, the consequences of these scenarios are determined along with their respective frequencies. Finally, the multitude of this scenario is integrated in order to create the risk profile of the system. The risk profile describes the level of the risk in question and considers how this will affect decision-making and corporate strategy.

The PRA process is covered in the risk management process, which includes risk identification and analysis. In PRA, risk control and review are not covered.

3-1-5 Multi Attribute Risk Assessment

Multi Attribute Risk Assessment (MARA) [15] is a technique for evaluating risk and for identifying and prioritizing both the set of threats and the security requirements.

Multi Attribute Risk Assessment considers many factors such as reliability, availability, safety and confidentiality that can be critical for a system. Each of these factors has its own risks, and hence it enables the analyst to find the right trade-off between these factors. This differentiates MRA from other risk assessment techniques which consider only certain factors (e.g., PRA considers only severity and likelihood).

The risk assessment process of multi-attribute risk analysis can be seen in Figure 3-4. In the first stage, threats are identified as potential risks and less harmful risks . After an initial set of threats is provided in order to initiate the risk assessment process, the security manager refines and orders the list of identified risks. The next step is to provide some attributes, such as lost revenue or productivity. The security manager estimates the distribution of attack frequencies and outcome attribute values for each threat. The next step is to rank each attribute by considering all of the attributes when choosing cost-effective countermeasures to deal with existing threats. In the final step, the results of the multi-attribute risk assessment are compared with the initial order. After the risk assessment is complete, risk mitigation measures are determined for each threat. The security manager focuses on the highest priority threat for the organization in order to mitigate it first.

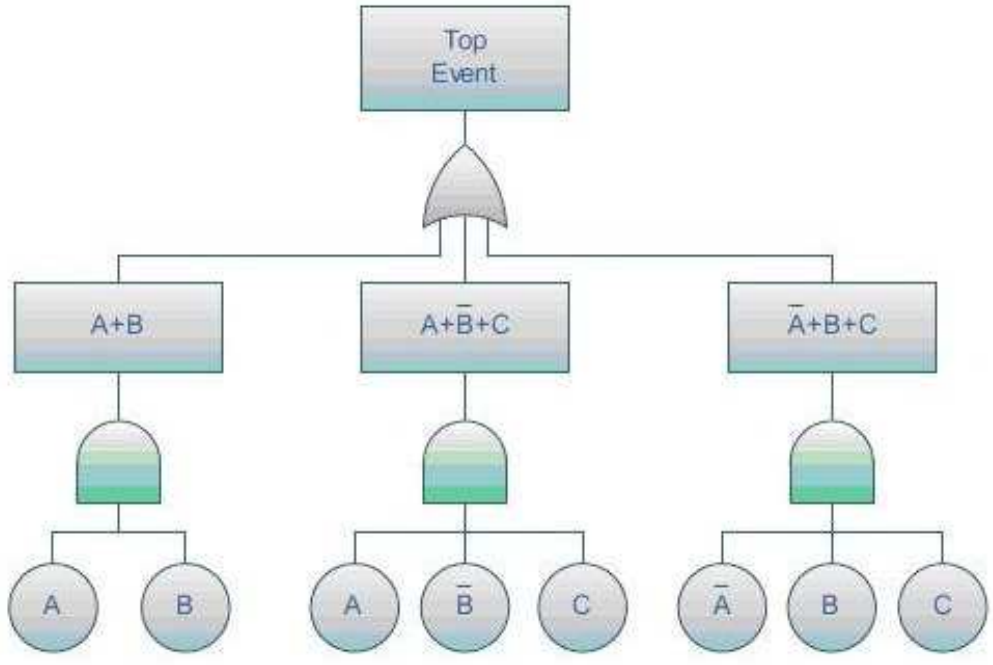

Figure 3-5: Fault Tree Notation

3-1-6 Fault Tree Analysis

Fault tree analysis (FTA) [16] uses fault tree notation to describe the causes of an event. Fault trees are very popular in risk analysis. Fault tree notation is used to specify the logical structure of a system and to support its assessment.

The root node of a fault tree depicts an unwanted incident or a failure. The root node is decomposed into different events called intermediate nodes and leaf nodes. The probability of the root node is the result of the probabilities of the leaf nodes and the logical gates *"OR"* and *"AND"*. In principle, a system can be divided into several sub-systems. In FTA, the root node and the intermediate root can depict this situation and the relationships between sub-systems can be *"OR"* or *"AND"*, depending on how the entire system works. Moreover, fault trees can be used both qualitatively and quantitatively. As a qualitative approach, FTA is used to specify the different paths that lead to the unwanted incident, while as a quantitative approach, it is used to estimate the probability of the incident described in the top node. An example of fault tree notation can be seen in Figure 3-5.

3-1-7 CORAS

The CORAS risk modeling language [3] is a customized graphical language that is used for the communication, documentation and analysis of scenarios involving security threats and risks. CORAS was designed based on UML in order to model security risk analysis.

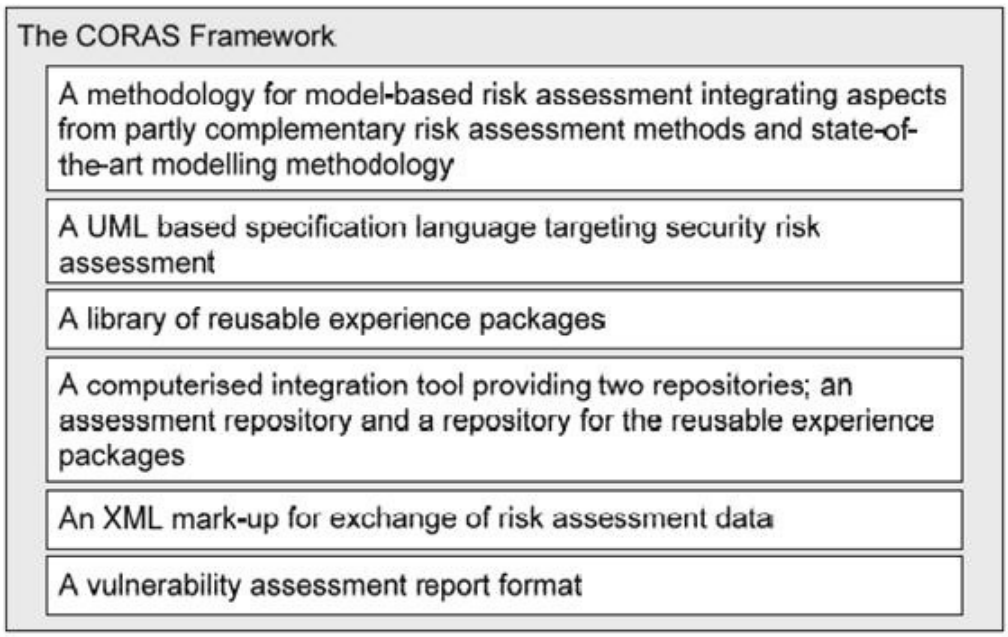

Figure 3-6: Coras Framework

The objective of CORAS is to help the analyst during the security risk analysis process. This method uses several international standards, such as AS/NZS4360, IEC60812 (FMEA/FMECA) [17] and (FTA) [16], and the process follows the Australian/New Zealand Standard for Risk Management. The CORAS method has five main phases, namely: (1) establish context; (2) identify risks; (3) analyze risks; (4) evaluate risks; and (5) treat risks.

With regard to the risk management process described in the previous section, the phrases of the CORAS method are quite similar. It starts by identifying the risk, which carries across two sections in CORAS: establishing the context and identifying the risk. The next phases are also similar to the risk management process: analyze risks and evaluate risks are both accommodated in the risk assessment process. The last stage in the CORAS method is risk treatment, which is considered to be a risk control process.

Every phase has a different purpose and produces different types of documentation. From its methodological approach and graphical language, the CORAS project resulted in a library of reusable experience packages, a computerized integration tool, an XML mark-up for the exchange of risk assessment data and a vulnerability assessment report format, as depicted in Figure 3-6. In the next chapter, the CORAS framework will be given in more detail.

3-1-8 GR Tropos

The GR Tropos goal model [2] has developed a formal framework for requirements analysis by refining stakeholders' interests and finalizing the elicitation of requirements by taking into account events (e.g., risk, opportunity) and treatments (e.g., tasks, countermeasure and mitigations).

The GR Tropos model represents requirements models as graphs (G, R) where G are nodes, which is comprised of three constructs: goal, task and event, and R are relations. The framework consists of three layers: the goal layer, the event layer and the treatment layer. The goal layer models the goals of stakeholders, while the event layer depicts uncertain event that will affect the goal layer. In the treatment layer, countermeasures are introduced in order to mitigate risk. A more detailed explanation of the GR Tropos framework will be discussed in the next chapter.

In summary, Table 3-2 will show the summary of previously discussed Risk Analysis Methods.

Table 3-2: Risk Analysis, Process and Method

Process/Methods	Risk Assesment			Risk Control		Risk Review	Risk Communications
	Identification	Analysis	Evaluation	Reduction	Acceptance	Events	
FMEA/FMEC	- Identify the functions, failures, effects, causes and controls for each item or process to be analyzed		- Evaluate the risk identified by the analysis	- Prioritize and assign corrective actions - Perform corrective actions and re-evaluate the risk		- Distribute, review and update the analysis, as appropriate - Risk priority numbers and criticality analysis	- Assemble the team - Establish the basic rules
HazOP	- Identify deviation using guide words on each element - Identify consequences and causes		- Repeat for each element and then each part - Identify protection, detection and indicating mechanism			- Re-study any parts of system	- Define scope, objectives and responsibilites - Select team
PRA	- Initial Events - Scenario Development - Frequency Evaluations		-	-			-
MRA	Threat Definition		Estimate Outcome Value	Compute Threat Indexes		Sensitivity Analysis	Justification from the manager
CORAS	- Identify Risks	- Analyze Risks	- Evaluate Risks	- Treat Risks			Establish context
Fault Tree	Identify all possible events as risk			-			-
GRTROPOS	- Find the alternative Solutions		- Evaluate Alternatives	- Asses the countermeasure to mitigate the risk			-

3-2 Legal Analysis

Nowadays there has been a rapid increase in government laws and regulations, industrial standards and company policies that need to be taken into account during the design of new organizational systems. These laws, regulations and policies may complement, overlap or even contradict one another because of different objectives and revisions [18]. Moreover, the meanings of words found in the relevant documents are not always clear and unequivocal. These laws, regulations and policies need to be analyzed during the definition of requirements for the new system. Logical representation enables users to identify unintended ambiguities in the text. This accords requirements engineers to identify specific ambiguities and to dissolve these issues before the system development process starts. There have been several efforts to model legal aspects that will be presented in the following section.

3-2-1 Symbolic Logic

One of the earliest efforts to model legislation introduced the use of symbolic [19] which is known as mathematical logic. This approach tried to balance the advantages of natural language with the exactness of symbolic logic, acting as a predecessor for later attempts to establish both human- and machine-readable interpretations. Allen's technique assigned six key logical connectives: implication, conjunction, complication, exclusive disjunction, inclusive disjunction and negation. By classifying these logical connectives, one can remove most of the unintended ambiguities present in legislative texts by using a more mathematical representation. A complete example can be seen in Table 3-3.

3-2-2 Deontic Logic

Generally, laws are intended to prescribe how the world should be and as such are related to their Deontic. Moreover, laws are very complex artifacts and are hard to capture because they are expressed in natural language and are intentionally vague in order to support as of yet unseen circumstances. Deontic logic [20] is a branch of modal logic that is described as the logic of prohibition, permission and the obligations to reason with regard to normative versus non-normative behavior. Obligation is defined as legal duty that an individual can be forced to perform or penalized for neglecting to perform. Permission is defined as the authority to perform an act which, without such authority, would have been unlawful, while prohibition is the act of prohibiting or the state of being prohibited.

If an actor j is obligated to perform an action (A), then the fact that j has an Obligation to carry out A can be expressed as $Obl_j(A)$.

If an actor j is forbidden to perform an action, he has a Prohibition, which is represented as $Forb_j(A)$, and can be written in terms of obligation as $Forb_j(A) = Obl_j(\sim A)$.

If an actor j is permitted to perform an action, then he as a Permission (predicate $Perm_j(A)$) which can be represented in terms of obligation as $Perm_j(A) = \sim Obl_j(\sim A)$.

Table 3-3: Symbolic Logic Example

CONNECTIVE	SYMBOL	EXAMPLES	
		ORDINARY VERBAL FORM	SYSTEMATICALLY PULVERIZED FORM
Conjuction	1. &2.	The six logical connectives dealt with here are conjuction, exclusive, disjunction, inclusive disjunction, negation, implication and coimplication	The six logical connectives dealt with here are 1. conjunction &2. exclusive disjunction &3. inclusive disjunction &4. negation &5. implication &6. coimplication
Exclusive disjunction	1. OR 2.	A person either understands them or he does not.	A person either 1. does OR 2. does NOT understand them
Inclusive disjunction	1) 2) &OR	Exclusive disjunction and/or inclusive disjunction may prove tricky for a while, but one soon learns to distinguish them.	1) Exclusive disjunction 2) &OR inclusive disjunction may prove tricky for a while, but one soon learns to distinguish them
Negation	NOT	The explanation here should not be hard to understand	The explanation here should NOT be hard to understand
Implication	1. 2.	If a person can read, then he should be able to understand it very easily	1. A person can read 2. HE SHOULD BE ABLE TO UNDERSTAND IT VERY EASILY
Coimplication	1. 2.	If, and only if, a person can read, he should be able to understand it very easily	1. A person can read 2. HE SHOULD BE ABLE TO UNDERSTAND IT VERY EASILY
1. Antercedent 2. CONSEQUENT			

3-2-3 Hohfeldian Legal Taxonomy

A conceptual language designed to capture legal prescriptions has been adopted from Hohfeldian legal taxonomy, which is grounded on eight elementary concepts classified by Hohfeld [21] as privilege, claim, power, immunity, and their correlatives no-claim, duty, liability and disability. The concept of correlativeness states that rights have a relational nature, such as claim-duty, privilege-no-claim, power-liability and immunity-disability. Two rights are correlatives when the right of person A implies the existence of person B (A's counterparty), who has the correlative right. Correlativeness involves two subjects: the owner of the right and the one, against the counterparty. These fundamental Hohfeldian legal rights are depicted in Figure 3-7.

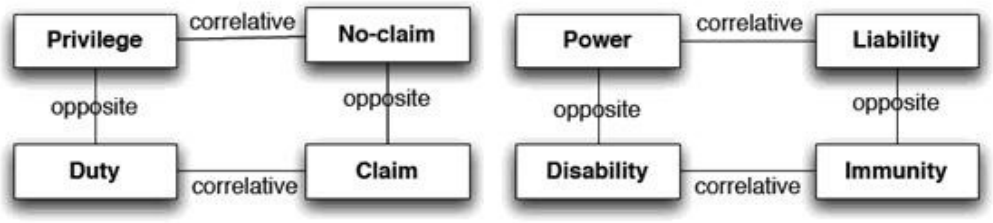

Figure 3-7: Hohfeldian Legal Right

- **Privilege**
  A privilege is an exemption from a duty, which is given to a particular person or group of people.
- **Claim**
  A claim is a legal action taken in order to obtain the enforcement of a right protected by law against another party.
- **Power**
  Power is the right, authority and ability to take action or accomplish acts.
- **Immunity**
  Immunity is an exemption from performing duties that the law generally requires other citizens to perform.

Table 3-4 shows the mapping of Hohfeldian's concept and deontic logic in terms of obligation. From the table, it can be seen that the term obligation is used to compare the expressiveness of deontic logic and the Hohfeldian concepts. Obligation as the center point of comparison can be used to express two other modal logics of deontic logic. Prohibition is presented as the obligation not to do something, and permission is expressed as not being obligated not to do something.

The four basic rights in Hohfeld's taxonomy can be presented using obligation. Duty is expressed as an obligation to carry out an action, while an obligation not to carry out an action is called disability. Privilege can be presented as the freedom to carry out an action or, in other words, as the lack of an obligation to carry out an action. Finally, the freedom to carry out an action that is forbidden is called power.

The only Hohfeldian concept that cannot be captured by deontic logic is privilege. In terms of obligation, privilege is equal to not being obligated to do something. This concept is needed when an actor has freedom, regardless of whether he wants to carry out an action or not. For example, giving a tip in a restaurant is a privilege, as the waiter cannot claim it. Therefore, deontic logic cannot capture all of Hohfeld's concepts, or in other words, Hohfeldian is more expressive than deontic logic in capturing law, as can be seen in Table 3-4.

Table 3-4: The Mapping of Hohfeldian and Deontic Logic

Term	Deontic Logic	Hohfeldian Concept
Obligation (x)	Obligation (x)	Duty
Obligation (∼x)	Prohibition (x)	Disability
∼Obligation (x)	Not Available	Privilege
∼Obligation (∼x)	Permission (x)	Power

3-2-4 NOMOS

NOMOS [4] is a framework that has been developed in order to model law. It is based on Hohfeld's fundamental legal taxonomy. NOMOS adopts i* [22] and extends it in order to model legal concepts in a goal-oriented modeling framework in order to help requirements analysts to address the problem of requirements compliance. It proposes a conceptual solution that combines elements of goal orientation with elements of legal theory, resulting in models of requirements compliance based on a model of law .

In NOMOS, the i* framework is used as a frame of reference for intentional modeling. i* is a modeling framework tailored to model a domain as being composed of heterogeneous actors with different goals. Actors depend on each other to undertake their tasks and achieve their goals. i* addresses two aspects of the domain: the strategic dependencies between actors and the strategic rationale of the actors. Through goal models, an alternative solution for the satisfaction of stakeholders' goals can be analyzed and chosen from among possible solutions on the basis of specific criteria. A detailed explanation of the NOMOS framework will be discussed in the next chapter.

Chapter 4

Legal Risk Analysis

In this section, the state-of-the-art frameworks will be discussed. GR Tropos, NOMOS and CORAS are described in detail in section 4.1. The implementation of the healthcare scenario using these frameworks is described in section 4.2. The lessons learned from implementing the scenario using these frameworks are explained in section 4.3.

4-1 Legal Risk Framework

Some frameworks have already been studied, such as GR Tropos [2] and CORAS [1] for modeling risk analysis, and NOMOS [4] and Extended CORAS [3] for modeling legal analysis. The discussion of each framework will be explained in this section.

4-1-1 GR Tropos

GR Tropos [2], an extension of Tropos [23], is a modeling language which is founded on the concepts of goal-based requirements adopted from the i* [22]. GR-Tropos provides a risk reasoning process for performing requirements analysis by identifing stakeholders' goals, identifying events, assess risks (e.g., risks and opportunities), and identifying treatments (e.g., tasks, countermeasures and mitigations). A descriptions of the process used in GR Tropos can be seen in Figure 4-1 [24].

1. **Goal Operationalization** is used to analyze the goals of actors. First, goals are identified and can be decomposed or given to other actors to be achieved. Hence, goals are used as input for goal refinement or goal dependency. Afterwards, using contribution analysis, the goals are analyzed.

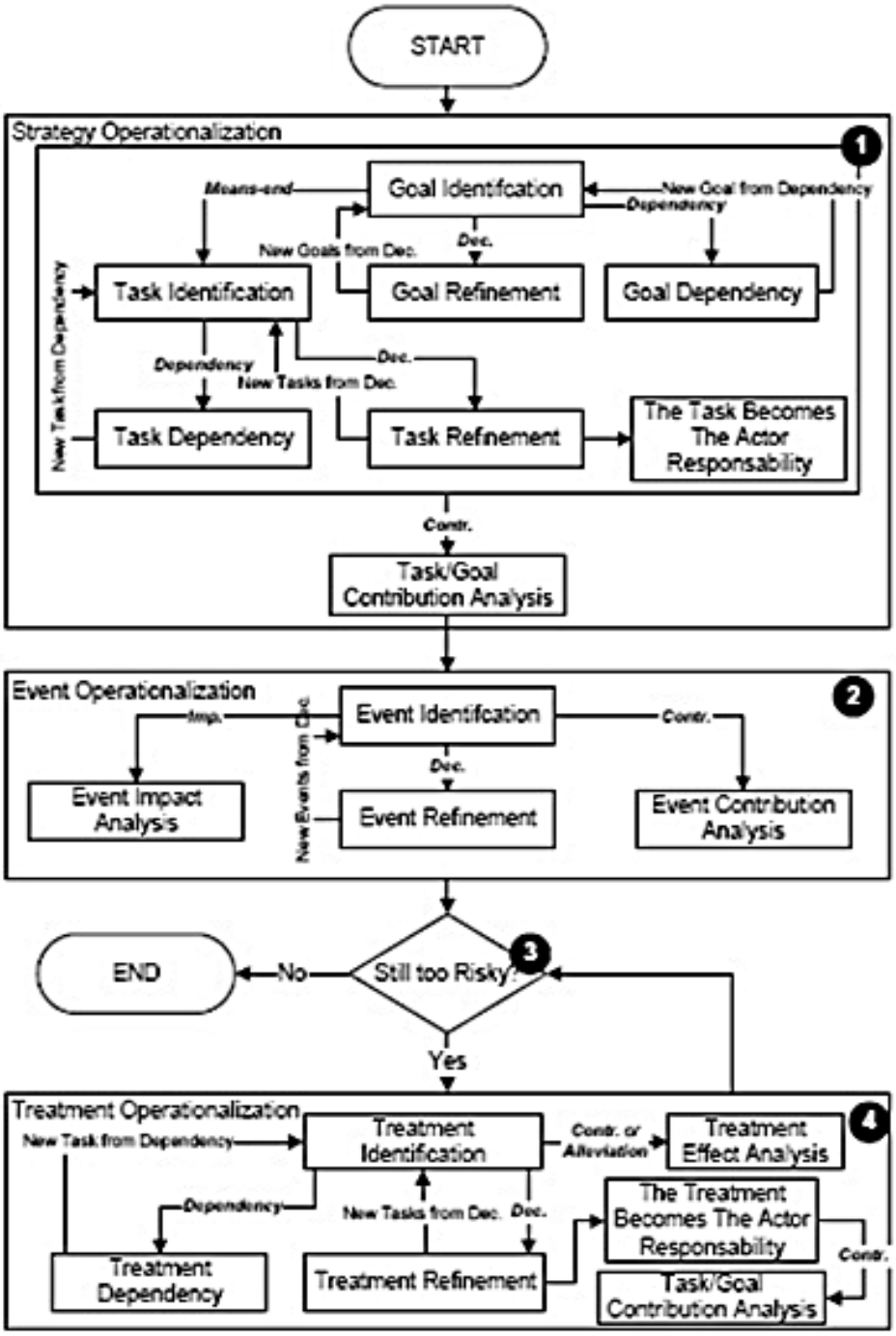

Figure 4-1: GR Tropos Process

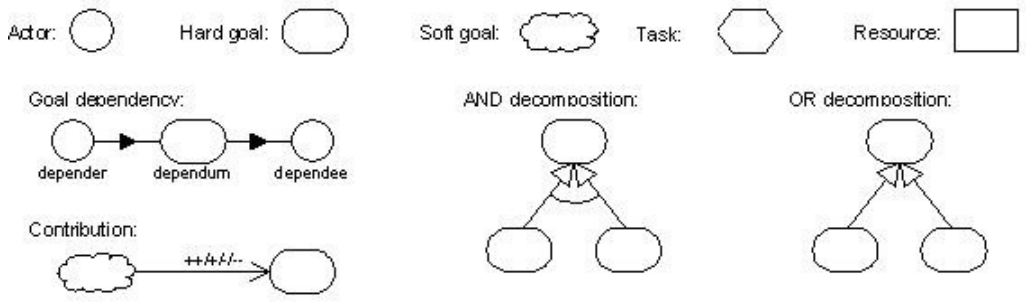

Figure 4-2: Tropos Notation

2. **Event Operationalization** aims to analyze events and their impact on the strategy layer. First, the events are identified and then analyzed through refinement and contribution analysis.

3. **Risk Reasoning** calculates the risk level perceived by each actor in the organization. This process is explained in detail in Algorithm 1.

4. **Treatment Operationalization** is used to refine the GR model when the risk level is higher than the risk acceptance level defined by the actors. First, treatments are identified and then, through contribution analysis, the influence of treatments on the strategy layer is modeled.

The GR Tropos model represents requirements models as graphs (G, R), where G are nodes and R are relations. G is comprised of three constructs: goals, tasks and events. The notation of the Tropos modeling element is depicted in Figure 4-2. These notations are used by GR Tropos with the addition of events, which are depicted as pentagons.

- **Actor**
  An entity that has strategic goals to be reached and tasks to be carried out. An actor is symbolized as a circle.

- **Goal**
  The objectives that have to be achieved by the actor. There are two types of goal, i.e., hard goals and soft goals, which are symbolized as ovals and clouds respectively. The latter have no distinct definition and/or criteria with which to decide whether or not they are satisfied.

- **Task**
  This represents the program of actions that is used to achieve goals or treat events. A task is also called a treatment and is symbolized as a hexagon.

- **Event**
  An event is defined as an uncertain circumstance which is out of the control of the

actors and that can have an impact on the achievement of goals. It is depicted as a pentagon.

- **Resource**
  A physical or an informational entity which is represented as a rectangle.

- **Dependency**
  A relationship between two actors, in which one actor (depender) depends on the other actor (dependee) in order to achieve a goal or carry out a task. The object between the depender and the dependee is called a dependum, which can be a goal, resource or task.

- **Contribution**
  The relationship between goals or tasks which depicts how and how much the goals or tasks can contribute to the fulfillment of the goal (either positively or negatively).

- **Decomposition**
  A relationship between goals or plans representing AND/OR decompositions.

Each entity of GR Tropos, as seen above, involves separate layers of conceptual analysis, namely the goal layer, the event layer and the treatment layer, as seen in Figure 4-3. The idea of separating the model into three layers creates a degree of flexibility in interconnecting the model language in each layer.

- **Strategy layer**
  The goal layer is used to refine the top goals into sub-goals and to analyze stakeholders' goals.

- **Event layer**
  The event layer is used to define the risks of the goal layer and to refine them.

- **Treatment layer**
  The treatment layer is used to introduce a treatment in order to mitigate the risks in the event layer.

Goals, events and treatments are all characterized by two attributes: SAT and DEN, which represent the value of the evidence that the goal can be satisfied and the value of the evidence that the goal can be denied, respectively. Their values are qualitatively expressed in the range of $(F)ull, (P)artial, (N)one$, with the intended meaning $F > P > N$.

R consists of AND/OR decomposition and contribution relations. AND/OR decomposition relations are used to refine goals, tasks and events in order to produce a finer structure. Contribution relations are used to model the impact of a node on another node. There are four types of contribution relation: $+$,$++$,$-$, and $--$. Each type of contribution relation can propagate either one type of evidence, SAT or DEN, or both types of evidence.

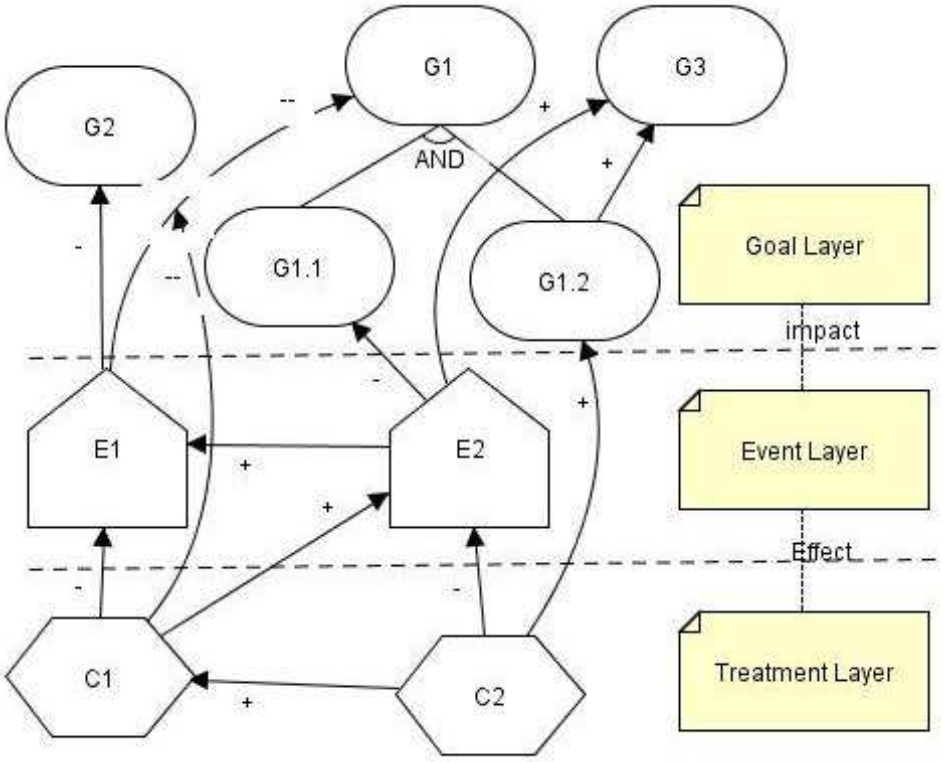

Figure 4-3: GR Tropos Framework

The risk reasoning process of GR Tropos can be seen in Algorithm 1 below. The reasoning starts by assigning the desired evidence values for top goals (i.e., satisfaction values, SAT, and acceptable risk values, DEN) and constraints (i.e., the level of conflict that is acceptable for the goal model and the minimum evidence value for a specific goal). Then, the reasoning process tries to find an assignment for leaf goals (input goals) that can satisfy the desired values.

Alg. 1 Risk Analysis Process

Ensure: analyse risk for each alternative solutions and find necessary countermeasures to ensure the satisfaction of top goals

Require: $goal\_model\ \langle \mathcal{G}, \mathcal{R} \rangle, label\_array, top\_goals, node\_array, input\_goals,$ $label\_array\ events$

1: $solution\_array\ solution$ {solution that has already encompassed risks and necessary countermeasures}
2: $alt\_solution \leftarrow Backward\_Reasoning(\langle \mathcal{G}, \mathcal{R} \rangle, \mathbf{nil}, top\_goals, input\_goals)$
3: $candidate\_solution \leftarrow Select\_Can\_Solution(candidate\_solution)$ $\{alt\_solution \subseteq candidate\_solution\}$
4: **for all** $\mathcal{S}_i \in candidate\_solution$ **do**
5: **if** $Satisfy(\langle \mathcal{G}, \mathcal{R} \rangle, top\_goals, \langle \mathcal{S}_i, events, \mathbf{nil} \rangle)$ **then**
6: $add(solution, \langle \mathcal{S}_i, \mathbf{nil}, Calc\_Cost(\mathcal{S}_i, \mathbf{nil}) \rangle)$
7: **else**
8: $boolean\_array\ Related\_Goals \leftarrow Related\_Goals(\langle \mathcal{G}, \mathcal{R} \rangle, \mathcal{S}_i)$
9: $labels \leftarrow Standard\_Forward\_Reasoning(\langle \mathcal{G}, \mathcal{R} \rangle, \mathcal{S}_i)$
10: $acc\_events \leftarrow Calc\_Event(labels, related\_goals, events)$
11: $nec\_treatment \leftarrow Backward\_Reasoning(\langle \mathcal{G}, \mathcal{R} \rangle, events, acc\_events, avail\_treatment)$
12: **for all** $\mathcal{T}_j \in nec\_treatment$ **do**
13: **if** $Satisfy(\langle \mathcal{G}, \mathcal{R} \rangle, top\_goals, \langle \mathcal{S}_i, events, \mathcal{T}_j \rangle)$ **then**
14: $add(solution, \langle \mathcal{S}_i, \mathcal{T}_j, Calc\_Cost(\mathcal{S}_i, \mathcal{T}_j) \rangle)$
15: **end if**
16: **end for**
17: **end if**
18: **end for**

Backward_Reasoning (line 2) generates a set of possible assignment values for the input goals that can satisfy the desired values of top goals which results in *alt_solution*

A subset of alternatives is chosen based on a certain criteria called *candidate_solution* in order to evaluate and choose from among all of the possible solutions (line 3). Then, every *candidate_solution* is examined against the risks and necessary countermeasures are introduced (lines 4-18).

If the *candidate_solution* does not need countermeasures to achieve the desired values for the top goals, then *candidate_solution* is added directly to the solution and its cost is calculated (line 6). Otherwise, countermeasures must be introduced in the *candidate_solution*

(lines 8-16).

The risk values that are acceptable to the stakeholders are calculated first so that countermeasures can be introduced in order to mitigate the risk. In other words, the maximum assignable risk values are discerned first in order to generate an acceptable DEN value for law goals.

Standard_Forward_Reasoning (line 9) is used to propagate the input values of the *candidate_solution* in the model and to evaluate the impact of the risk. Once an assignment has been made for all of the goals in the model, then the acceptable values for the event can be calculated (i.e., values that can still satisfy the desired law goals) using the *Calc_Event* procedure.

In order to find possible treatments that can guarantee acceptable levels of risk (*acc_event*), *Backward_Reasoning* is used. Finally, in lines 12-16, every set of treatments is examined with regard to the initial desired values and affordable costs. In order to do so, the $Satisfy$ algorithm in line 13 is used.

4-1-2 NOMOS

NOMOS [4] is a modeling language which defines the set of requirements to comply with the law and harmonizes the law and stakeholders' interests. NOMOS proposes the concept of intentional compliance, which means that if every actor reaches its goals, then the law is respected. Based on that concept, general rules can be derived to define the notion of requirements compliance. Given a set of requirements represented as the goals of the actors R and a set of domain assumptions D, then if the requirements are compliant with a law L, this is written as $R, D \models L$. If, for every possible state of the world, R holds, then L holds.

The NOMOS modeling language conceives law as a partially ordered set of normative propositions (NP). In principle, legal prescriptions can be subdivided into their most basic atomic element, which is called NP. The basic element of an NP is the Hohfeldian concept of rights as having a dual nature, which means that two rights that connect describe the same reality, but from two different points of view. This results in four classes of rights, namely Privilege-No-claim, Claim-Duty, Power-Liability and Immunity-Disability. Rights have two domain actors, which are the right holder and its counter-party. If a set of normative propositions $\{NP_1 \dots NP_n\}, NP_k > NP_{k+1}$, if NP_k is satisfied, then the fulfillment of NP_{k+1} is not relevant. The concept of a relationship based on dominance is introduced in order to specify the relationship between actions, represented as a link between two prescribed actions and labeled with a " $>$ " symbol that goes from the dominant action to the dominated one.

The visual notation of NOMOS helps the requirements analyst to work with legal prescriptions. NOMOS notation is also adapted from the i* framework of visual notation that has already been explained as part of the description of Tropos visual notation given above.

Figure 4.4 depicts the notation of the NOMOS language. As in GR Tropos notation, the actors are modeled as circles. These two actors act as the holder and the counterparty and are linked by a specified action right that is modeled as a triangle. The various kinds of rights, which are Privilege-No-claim, Claim-Duty, Power-Liability and Immunity-Disability, are indicated with labels on both edges of the right relationships. Based on the Hohfeldian fundamental legal taxonomy, these rights have a correlative relationship, which means that if one actor holder asks its counterparty to carry out an action, then the counterparty has an obligation to fulfill it. Each right within NOMOS notation can be described as follows:

- **Power-Liability**
  The correlative of power is liability. The holder with power is in a position to affect the legal relations of the counterparty. For instance, in many countries, courts have the power to terminate parental rights and to transfer them to the social welfare authorities.

- **Privilege-No Claim**
  The Privilege-NoClaim correlative means that if the holder has a privilege over the counterparty with regard to a specific action, the counterparty has no claim against the holder. For example, if an individual has the right to stay in certain country then this is a privilege. It means that the government has no claim against him or her and cannot make him or her leave the country.

- **Claim-Duty**
  For Claim-Duty correlatives, if the holder has the claim against the counterparty with regards to do something, then the counter-party will have the duty to the holder to fulfill it. For example, if person B owes 100 euro from person A, then person A has a claim right against B to returned 100 euro.

- **Immunity-Disability**
  The Immunity-Disability correlative can be described as follows. If the holder is immune against the counterparty, the counterparty has no power over the holder's rights. For example, diplomats are supposed to have diplomatic immunity. If they commit a crime in their host country, they are immune against legal prosecution.

Compliance with the law in NOMOS involves two level of analysis: an atomic level, in which the individual actor has to comply with the law, and an aggregate level, which takes into account the relationships between actors.

Atomic Compliance
Atomic compliance means that an actor does what laws tell him to do. Taken from NOMOS atomic compliance, compliance condition as a function R such that it is true if, given an

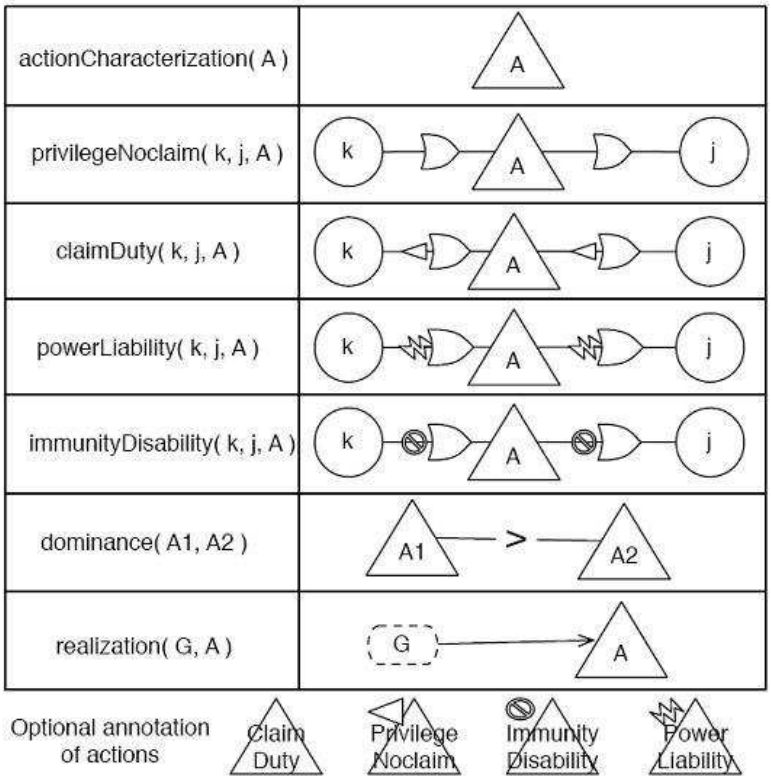

Figure 4-4: Nomos Notation

NP, an actor j either does not have to comply, or has to comply and actually complies. At the atomic level, compliance is ensured if R is equal to true .

$$R(j, NP) = \neg\, needToComply(j, NP) \vee comply(j, NP) \tag{4-1}$$

At the atomic level, compliance is ensured if R equals to true.

Aggregate Compliance
In aggregate compliance, an actor is compliant with a law L if it is compliant with every normative proposition of that law. Formally, compliance occurs if for any normative proposition NP addressing an actor j, there exists a goal G that fulfills NP. Therefore, aggregate compliance C exists if:

$$\forall NP \in L, R(j, NP) = true \tag{4-2}$$

Compliance Rules.
From the atomic compliance and aggregate compliance equations given above, the set of NOMOS rules below has been defined in order to check compliance.

- **Rule 1. Abilities.**
  If an action has to be realized by an actor, then the actor must have at least one goal that realizes the action. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

- **Rule 2. Decomposition**
  If a goal G represents the ability of an actor to realize a certain NP, then for each sub-goal of G, by achieving that sub-goal, the NP must still be realized. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

- **Rule 3. Contribution**
  If a goal G represents the ability of an actor to realize a certain NP and the goal is the target of a contribution, then by achieving the contribution of the source goal, the NP must still be realized. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

- **Rule 4. Delegation**
  If a goal is (a part of) the ability of an actor to realize a certain NP and it is delegated to another actor, then Rule 2 must hold for the delegatee. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

- **Rule 5. Duty**
  If a N is a duty which specifies that an action must be performed by a specific actor, then the action must be realized by the actor.

- **Rule 6. Privilege, Claim and Power**
  If an actor has a claim, then the actor can discretionally decide to realize the claim through the use of an ability. Note that these rights are different from each other for the counterparties, but as they are only somewhat different for the holders, we will not draw such distinctions here.

- **Rule 7. Liability and Immunity**
  If an actor experiences a liability, such as a sanction, it may want to prevent the sanction from being applied by searching for immunity. In this case, realizing this immunity overcomes the liability.

- **Rule 8. No-claims and Disability**
  If an actor experiences a no-claim or a disability, then the action cannot be realized.

4-1-3 CORAS

The CORAS modeling language [25] supports the security analyst during the phases of security risk analysis (i.e., context establishment, risk identification, risk estimation, risk evaluation and treatment identification). CORAS is used to apply several risk analysis techniques in an integrated manner, and also to perform different services during each phase of analysis. The notations used in the model are defined as follows:

- **Stakeholders**
  Stakeholders are persons who perform an activity which concerns the target of the evaluation. These stakeholders can act as one of two types of threat agent: deliberate and accidental threat agents. The other type of threat is a non-human threat, which is caused by other technical aspect that could harm assets;

- **Vulnerability**
  Vulnerability is a weakness of the system that could be exploited and may result in a security breach, a violation of the system or other effects;

- **Threat Scenario**
  A threat scenario is a potential cause of an unwanted incident. Threats may exploit vulnerabilities and cause an incident which will reduce the value of one or more assets;

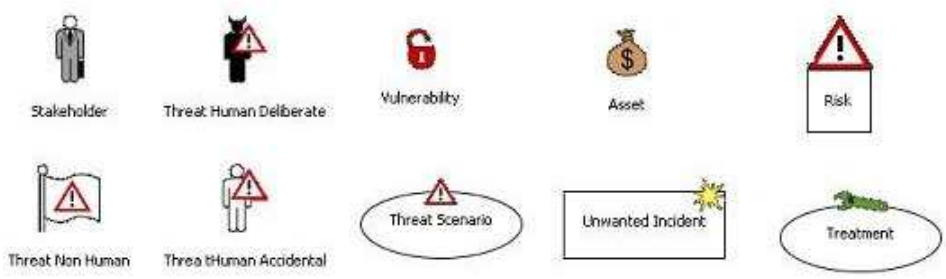

Figure 4-5: Coras Notation Model

- **Asset**
  An asset is something that a stakeholder directly assigns a value to, and therefore it is protected from being compromised;
- **Unwanted Incident**
  An unwanted incident is an event that may harm assets and must preferably be prevented. In other words, an unwanted incident is the result of a threat exploiting a vulnerability;
- **Risk**
  A risk is defined as an unwanted incident, along with its estimated likelihood and consequence values;
- **Treatments**
  Treatments represent various actions designed to reduce risk.

The UML use case notation has its own set of standardized icons, but the UML profile is recognized by its specialized graphical icons that depict the different terms in the conceptual model. The icons are used to make the models easier to read and understand. Figure 4-5 shows the CORAS notation.

The CORAS language provides a number of specialized UML diagrams to support threat modeling, such as asset diagrams, threat and unwanted incident diagrams and treatment diagrams.

- **Assets Diagram**
  Asset diagrams are used to present an overview of the assets and to exhibit the relationship between assets and stakeholders, as well as their interest in the assets.
- **Threats and unwanted incidents Diagram**
  Threat diagrams are used to present the chains of events which are initiated by threats and that have consequences for the assets. A threat agent initiates a threat scenario that leads to an unwanted incident.

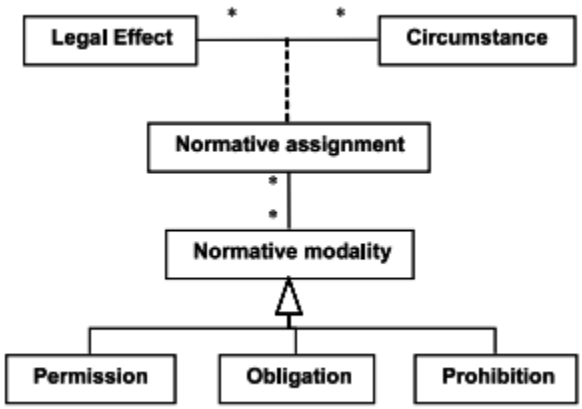

Figure 4-6: Normative Modalities

- **Treatments Diagram**
  When threats have been identified and analyzed, the next step is to introduce treatments which may have different effects on risks. They may reduce the consequences or frequency of the unwanted incident, or transfer the risk to another party.

Extended CORAS

Extended CORAS [1] is used to model legal aspect of legal risks based on the idea of modal logic [20]. This logic is used to express which activities are permitted, obligatory or forbidden. Normative modalities are used in deontic logic to describe normative status. Normative modalities are used in the relationship between legal effects and circumstances in order to specify which circumstances are permitted, obligatory or forbidden by the legal norm in question, as can be seen in Figure 4-6. Legal reasoning leads to legal criteria based on the relevant source material, such as statutes and regulations.

Legal norms which describe legal requirements and consequences are the focus of legal risk analysis in CORAS. Legal norms are generally structured in the form of an antecedent and a consequent: if A then B. The antecedent describes the criteria for the norm to apply, while the consequent indicates the legal effects of the norm being applied. The legal impact of a particular norm on an actor depends on the activity being performed as well as the role that the actor plays. Therefore, a circumstance consists of an actor, an activity being performed by that actor and the role which the actor plays while performing the activity, as depicted in Figure 4-7.

In legal risk analysis, parts of the target of evaluation will originate from legal issues formulated in legal texts such as laws and contracts. The practice of modeling legal issues is focused on modeling the effects of the appropriate legal texts, and not on modeling the legal texts themselves.

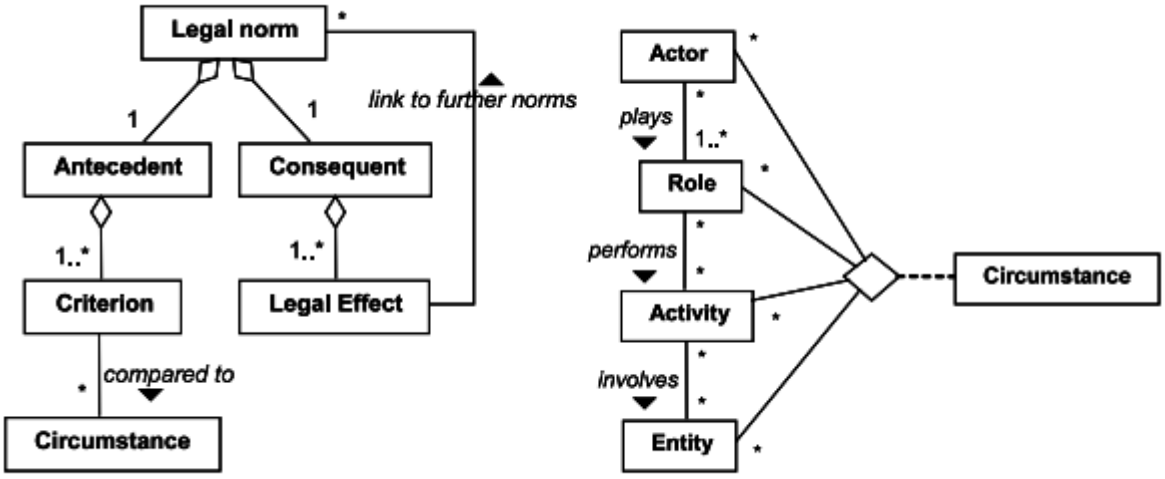

Figure 4-7: Legal Norm and Circumtance

4-2 Scenarios applied to the Framework

In this section, the healthcare system scenario that was discussed in Chapter 2 will be implemented in GR Tropos, NOMOS and CORAS.

4-2-1 GR Tropos

As a goal-oriented framework, GR Tropos models the scenario by focusing on the goals of each actor. Figure 4-8 depicts the healthcare system scenario, in which all goals are symbolized as rounded rectangles. The goal of the Patient is to be able to obtain medical services. This goal is decomposed into two sub-goals, which are Get Medical Treatment and Get Insurance Assistance. In order to fulfill this goal, the Patient must share his or her information to the PHR provider. The Patient and the PHR Provider are actors, and are therefore depicted as circles. In the GR Tropos model, the fulfillment of the goal is affected by risk, which is represented as an event that may occur. In this case, the risk Data Misused obstructs the fulfillment of Provide PHR Info goal. A risk is represented as a pentagon and has a negative impact on the goal. One of the ways to mitigate the risk is by introducing a treatment (depicted as a hexagon). The Privacy Policy treatment is used so that the Patient's medical information will not be misused. As a result of the Privacy Policy treatment, Patients will know beforehand for what purpose their data will be used.

The PHR Provider has a goal, namely Provide Medical Service, that can be decomposed into three goals, which are Manage PHR Info, Treatment Service and Payment Service. The information that is managed by the PHR Provider must be accurate, as the information will be shared with the other actors who need it. For example, if Patients want to get

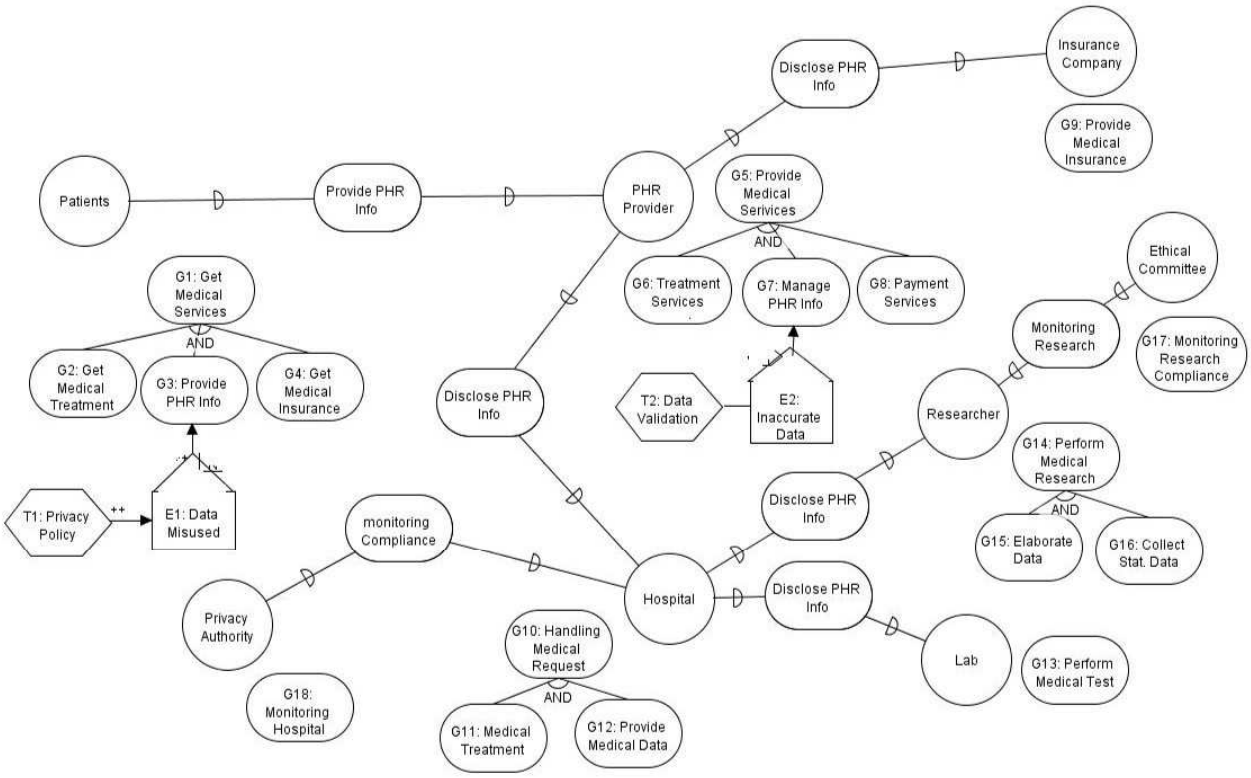

Figure 4-8: GR Tropos Model

Insurance Assistance, then PHR Provider will share Patients' personal information to the appointed Insurance Company, or PHR Provider will share Patients' medical info to the Hospital if Patients want to get Medical Treatment. Manage PHR Info has a risk that the data might be inaccurate. This risk is mitigated by implementing the Data Validation treatment.

In cases in which Patients need medical tests, then the Hospital will share the Patients' medical information with the Lab which will perform the outsourced Medical Tests. The Hospital will also share the Patients' medical data with the Researchers for research purposes. In order to monitor the research process, an Ethics Committee monitors the Researchers. In order to ensure compliance, a Privacy Authority monitors the Hospital. Take Hospital as an actor. Start setting the desired values for goals G_{10} with fully satisfy ($Sat(G_{10}) = F$) without any risk ($Den(G_{10}) = N$) and taking number of goals G_{11} and G_{12} as possible candidates.

In order to fully satisfy G_{10}, the only alternative solution is $\{G_{11}, G_{12}\}$ called candidate solution (line 3).

The candidate solution is now evaluated against risks. Since there is no risk that is associated to them therefore they are considered as solution. It means that the top goal is satisfied, with the value of top goal is ($Sat(G_{10}) = F, Den(G_{10}) = N$).

As GR Tropos is designed to model goals and risks, it cannot capture the legal aspect of the scenario. For example, based on the Directive, once Patients share their PHR Info, they will automatically have three rights (the right to be informed, the right to access, the right to object), as medical information is considered to be sensitive data. In this model, GR Tropos cannot model these rights. The duty to share PHR Info is modeled with a dependency goal model, while the other three rights cannot be captured.

4-2-2 NOMOS

NOMOS which is also based on goal oriented language as GR Tropos, also presents the PHR data protection scenario by concentrating on the goals of each actor. In NOMOS, the actors and goals are presented using the same symbols as in GR Tropos: actors are depicted as circles and goals are presented as rounded rectangles. NOMOS, which is designed for law modeling, is already equipped with a legal tool, and therefore it is easier to model legal aspects. The goals of every actor are modeled in the same way as in GR Tropos.

In this scenario, Patients assign ClaimDuty to the PHR Provider of their information (*ClaimDuty*(Patients, PHR Provider, Provide PHR Info)). Based on the Directive, once Patients share their PHR Info, they are granted three rights (i.e. the right to be informed, the right to access, the right to object). These rights are captured easily in NOMOS using Power rights. (*PowerLiability*(Patients, PHR Provider, Right to Info), *PowerLiability*(Patients, PHR Provider, Right to Access), *PowerLiability*(Patients, PHR Provider, Right to Object)). Patients share their Info with the PHR Provider in order to

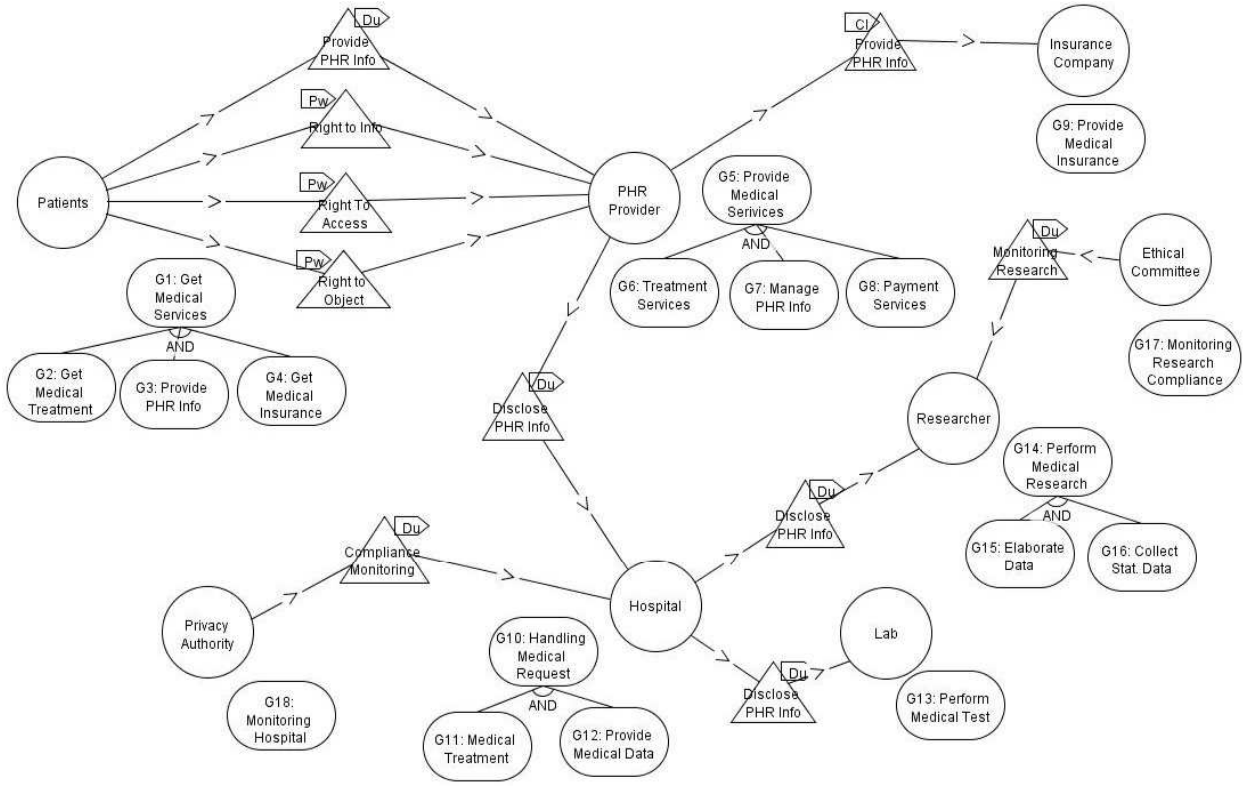

Figure 4-9: NOMOS Model

fulfill their goals (i.e. to get medical treatment and insurance assistance). Insurance assistance is performed by the Insurance Company, and therefore the PHR Provider has a duty to disclose Patients' Info to the Insurance Company. (*ClaimDuty*(PHR Provider, Insurance Company, Disclose PHR Info)). The PHR Provider also has a duty to the Hospital when Patients need medical treatment (*ClaimDuty*(PHR Provider, Hospital, Disclose PHR Info)). When the Hospital outsources medical tests, the Hospital also shares the Patients' Info with the Lab (*ClaimDuty*(Hospital, Lab, Disclose PHR Info)). The other actors who are given a claim by the hospital are Researchers (*ClaimDuty*(Hospital, Researchers, Disclose PHR Info)). Researchers have a responsibility to carry out scientific research in order to fulfill their goal. The Ethical Committee has a duty to monitor The Researchers with regard to the research that is being conducted (*ClaimDuty*(Ethical Committee, Researchers, Monitor Research)). The Privacy Authority also has a duty to monitor the hospital's compliance with the law (*ClaimDuty*(Priva, Hospital, Disclose PHR Info)). The model in NOMOS can be seen in Figure 4-9.

From the model, it can be seen that NOMOS only models the goals of the Actors. In contrast to GR Tropos, which considers risks and treatments in the model, the NOMOS model does not capture these constructs. For example, in the scenario, goal fulfillment is not affected by risk. The risk of Inaccurate Data cannot be modeled, and therefore if it

occurs, NOMOS could not detect it. Based on the Directive regarding data quality (i.e., Article 6), if data are inaccurate then this means that the law has been violated. NOMOS as a law modeling tool cannot detect violations of the law with regard to risks. If the model is not compliant with law, therefore the algorithm exists returning a failure (i.e., an empty set). If the function returned a non-empty set, this is in turn returns and the algorithm ends.

4-2-3 CORAS

In CORAS, the scenario is modeled in Figure 4-10 and Figure 4-11. In contrast to the two previous tools, CORAS is an asset-oriented language and is focused on the protection of these assets, which consist of the PHR information, depicted as a sack with a dollar sign. The six main actors can act as stakeholders and can also act as threat agents. Patients act as stakeholders who provide their PHR information to the PHR Provider, which can also act as a threat agent if it accidentally gives out incomplete or incorrect data: this would also be considered as a threat scenario.

The other actors, which are the Lab, the Hospital, the Researcher, and the Insurance Company, could also perform as deliberate threat agents which endanger the asset by selling it to a third party. The other possible threat scenarios are the deletion/alteration of PHR info and increased insurance rates, which would be caused by the Lab and the Insurance Company respectively. The alteration of PHR info is a violation of Article 6 of the Directive which defines data quality. The Researcher could also act as threat agent by keeping more medical information than is needed for research purposes, which would also violate Article 6 of the Directive. As an accidental threat agent, the Hospital could violate the Data Protection Law by breaching the patients' PHR info. The other two actors, the Privacy Authority and the Ethics Committee, which only act as stakeholders, have a duty to monitor the compliance of the hospital and the researchers respectively. This acts as a treatment.

4-3 Lesson Learned

The experience of implementing the healthcare scenario in CORAS, GR Tropos and NOMOS has highlighted the differences between these three frameworks. The findings can be grouped into three categories, namely graphical notation, law modeling and design focus. The idea behind grouping the findings is to explore the distinctive features of each framework. For instance, CORAS excels its design in graphical model , while NOMOS focuses on the legal analysis and GR Tropos focuses on the risk analysis process.

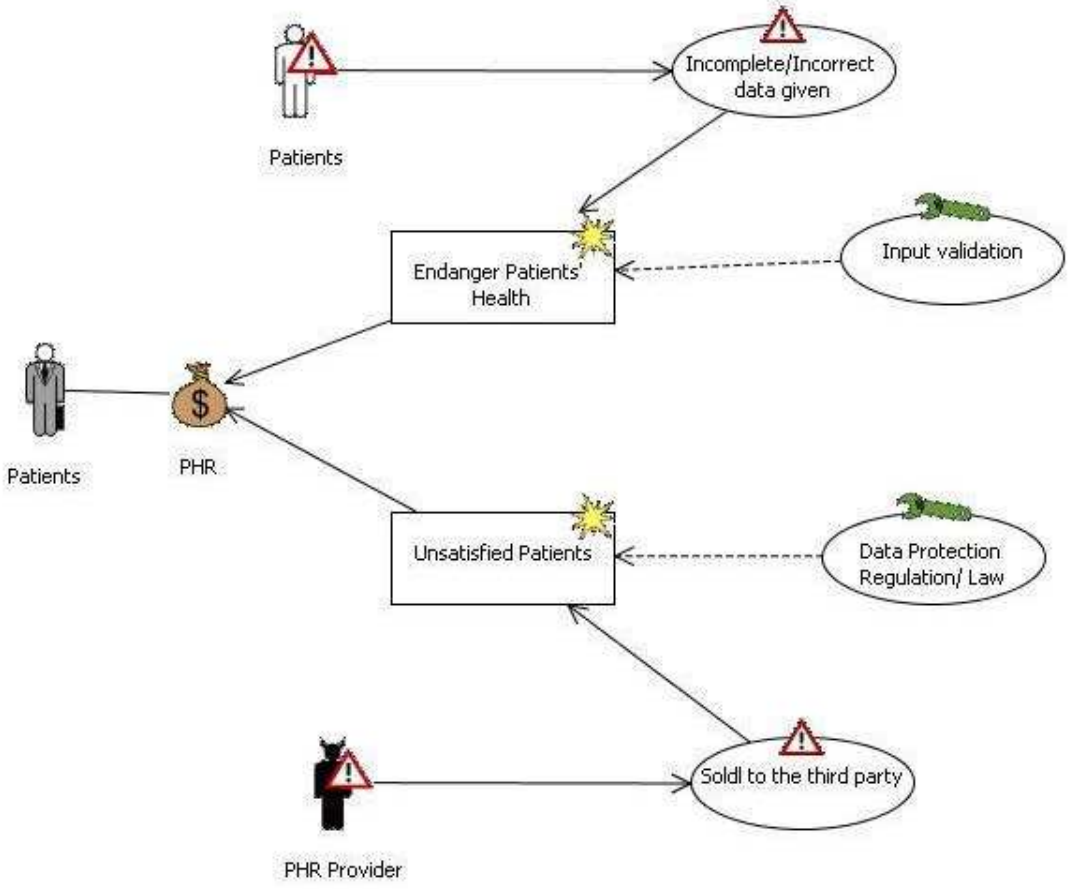

Figure 4-10: Coras Model - 1

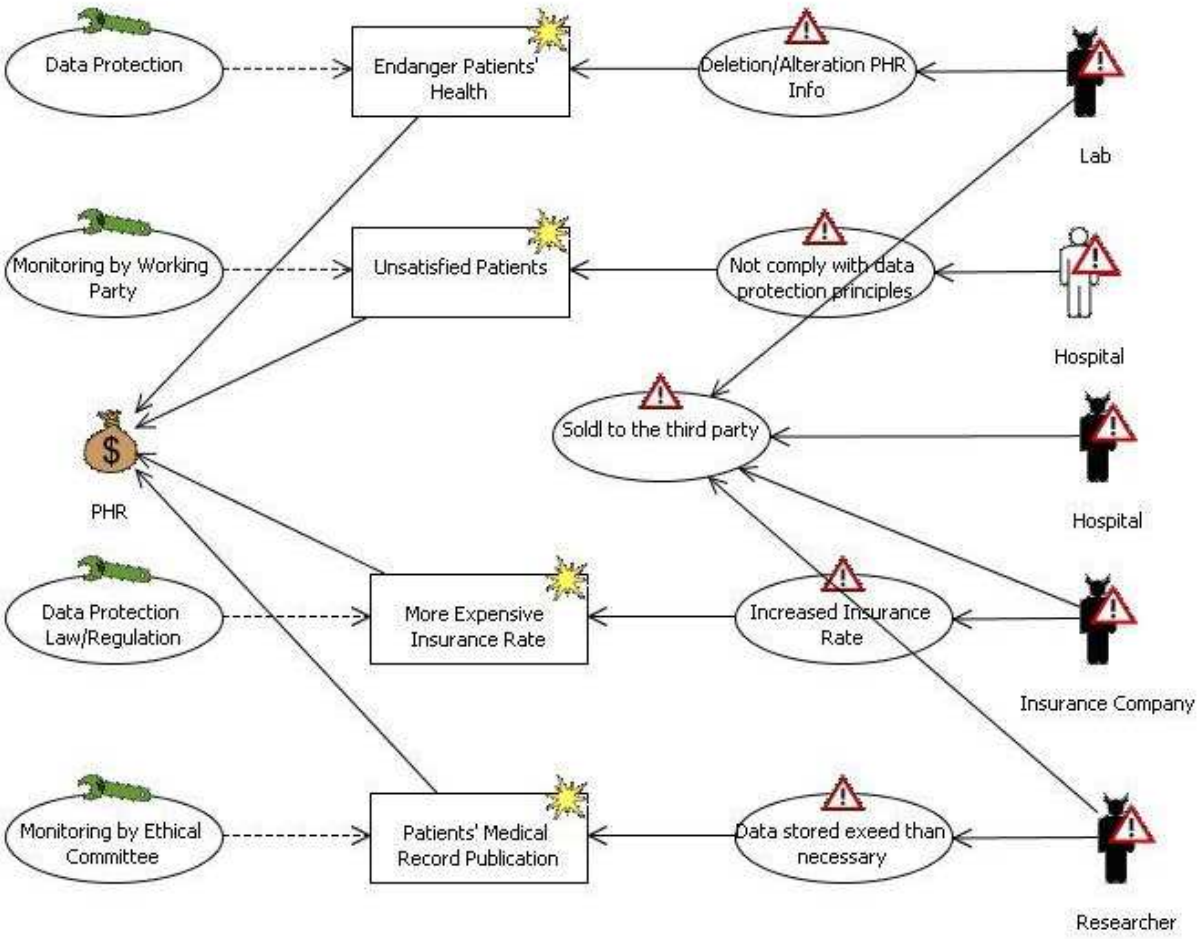

Figure 4-11: Coras Model - 2

4-3-1 Graphical Notations

Graphical notation encompasses the symbols and graphical presentation of each framework. The design of the symbols in each tool is different, as they are represented from a different point of view.

Although the CORAS symbols are representative, this comes at a cost. CORAS is an expensive modeling language as its symbols are redundant. For example, the two types of attacker, namely deliberate attackers and incidental attackers, could be modeled as one unit - an attacker. The division of the symbol for an attacker is useless as it has no added value with which to improve the risk management process.

Taken from a different perspective, the graphical notations in NOMOS and GR Tropos are simpler than those in CORAS. The symbols in both NOMOS and GR Tropos are two-dimensional geometric shapes, e.g., actors and goals are represented as circles and rounded rectangles, respectively. This representation is easier than the CORAS representation for use when modeling a complex scenario. Therefore, the scenario is easier to analyze. On the other hand, it is hard for users to understand the meaning of the symbols without learning the frameworks beforehand. Moreover, it is harder for users who are not familiar with risk analysis.

4-3-2 Law Modeling

Modeling the law is the most important part in this work since it deals with data protection directives that will be applied. Law modelling in these frameworks is also based on different concepts of law.

CORAS models law based on the concept of Deontic logic. As discussed in the previous chapter, modeling using Deontic logic has several limitations which prevent it from fully capturing the concepts of law. CORAS can model three actions, which are *"allow"*, *"forbidden"* and *"own"*, while other actions such as *Privilege* cannot be modeled. For example, in Scenario 1, in which the Patients provides information to the PHR Provider, the Patients uses *"forbidden"* and *"allow"* to model information sharing between these two actors, while *"own"* is used for actions directed toward the actor himself or herself, i.e., the Patient owns the asset, which is PHR Info.

The concept of law in NOMOS is based on the work of Hohfeld. Hohfeld offers more complete ways in which to capture laws, such as Duty, Disability, Privilege and Power, meaning that the law can be modeled in full. Privilege is the feature of Hohfeld's taxonomy that is not covered by Deontic logic.

Taking the same scenario as an example, when a Patient provides his or her PHR Info to the PHR Provider, NOMOS has two ways of modeling this scenario, using ClaimDuty and Privilege No Claim. When Patient has Privilege to the PHR Provider to share their information, the PHR provider has no claim toward the Patient. This means that the

Patient is free to share his or her information with the PHR Provider if he or she wishes. The other option is that when the Patient has claim to the PHR provider to share his or her information, then the PHR provider has a duty to fulfill it, and this implies that Patient has no freedom, whether they want to share their information or not.

These two models (i.e., Privilege and Duty) can be distinguished easily in NOMOS, whereas in CORAS, Patients can only use *"allow"* to share their information with the PHR Provider. As NOMOS offers more complete features with which to capture and model the law than CORAS, our proposed legal risk analysis framework will be based on NOMOS as the basic framework for modeling the law.

4-3-3 Design Focus

In this subsection, the design focus will be discussed, which refers to the basic design idea behind each framework. In principal, the design of these three tools is different: CORAS is designed based on an asset-oriented framework, while GR Tropos and NOMOS are based on goal-oriented frameworks.

As CORAS is an asset-oriented framework, the design focus of CORAS is on how to protect the asset from the threat and also on how to mitigate this threat by providing a treatment. Actors in CORAS are independent from the others. Moreover, an actor can be used to model either an asset owner or an attacker. From experience, it is hard to create a complete scenario, as there is usually a dependency relationship between the actors and other elements.

Basically, GR Tropos and NOMOS are extended forms of the Tropos language, which is a goal-oriented language. These two frameworks focus on the goals that must be achieved by each actor. The difference between GR Tropos and NOMOS lies in risk modeling. GR Tropos can model treatments and events, whereas NOMOS cannot model either.

In order to illustrate the distinction between asset-oriented frameworks and goal-oriented frameworks, we will adopt the scenario described in the previous subsection (Scenario 1) as an example, in which Patients share their personal and medical information with the PHR Provider.

When modeling this scenario in CORAS, the goals of Patients and the PHR Provider are not modeled. CORAS emphasizes in modeling the assets, which is PHR Info. This asset is protected against the threat scenario which is caused by two different types of attacker (intentional attackers and deliberate attackers). A treatment scenario is also provided in this model in order to mitigate the threat and to prevent the assets from being lost.

In case for the same scenario, NOMOS and GR Tropos will model this scenario different from CORAS. Focusing on the goals of each actor, NOMOS and GR Tropos model the goals of Patients and the PHR Provider explicitly. Moreover, the dependency relationship between the Patients and the PHR Provider is also modeled which shows that the achievement of Patients' goals depends on the PHR Provider and vice versa.

As previously stated, the threat scenario that may occur is not modeled, as well as the treatment to mitigate the risk in NOMOS. GR Tropos can capture the scenario in a more complete manner. GR Tropos uses an event to model a threat scenario. Another approach that is adopted by GR Tropos is by using a treatment to mitigate the risk. This approach is quite helpful to solve the problems of modeling the threat and its attacker.

Based on the above evaluation, it shows that GR Tropos is equipped with treatments and events to model risks. Therefore in our proposed legal risk analysis framework, GR Tropos is taken as the basis for modeling risk analysis. Although CORAS can model risk, GR Tropos has been adopted instead of CORAS since GR Tropos is a goal-oriented framework that is easier to be integrated with NOMOS as the basis for modeling law, as it is also a goal-oriented framework.

As already discussed in subsections 4.3.2 and 4.3.3, our proposed legal risk analysis framework will be based on the integration of NOMOS and GR Tropos. NOMOS will be used as the basis for modeling law, as it has more complete features for capturing laws, while GR Tropos will be used as the basis for modeling risk, as it is equipped with treatments and events. The integration of NOMOS and GR Tropos is very easy to be done since both of them are goal-oriented frameworks.

Chapter 5

Proposed Framework

Our proposed legal risk analysis framework is based on the integration of NOMOS and GR Tropos. NOMOS is used as the basis for law modeling, while GR Tropos is used as the basis for risk modeling. The integration of NOMOS and GR Tropos is easy to do since both of them are goal-oriented frameworks. Section 5.1 will discuss the meta-model and graphical notation of the proposed framework. Legal risk reasoning for the purpose of legal risk analysis will be discussed in section 5.2.

5-1 Meta-model and Graphical Notation

The NOMOS framework [4] is a modeling language that supports the representation of intentional and normative elements. The NOMOS framework concerns the verification of compliance with the law in software requirements by combining a law model with an intentional model of requirements. For intentional modeling, the i* [22] framework is used as a frame of reference. The i* is a modeling framework which is tailored to domains composed of heterogeneous actors with different goals. However, i* does not consider the risks which occur during the requirements analysis and it is not possible to analyze the effects of unpredictable situations on the stakeholders' goals.

The GR Tropos framework [2] is used to model and to reason risk within the requirements engineering process. It proposes risk analysis during the process of evaluation and the selection of alternatives.

In this work, a proposed framework for assessing legal risk has been developed by combining NOMOS and GR Tropos. The proposed framework introduces a-three-layer model, in which risks are related to goals and countermeasures by incorporating new primitive events and treatments. A risk is an event that has a negative impact on the satisfaction of a goal,

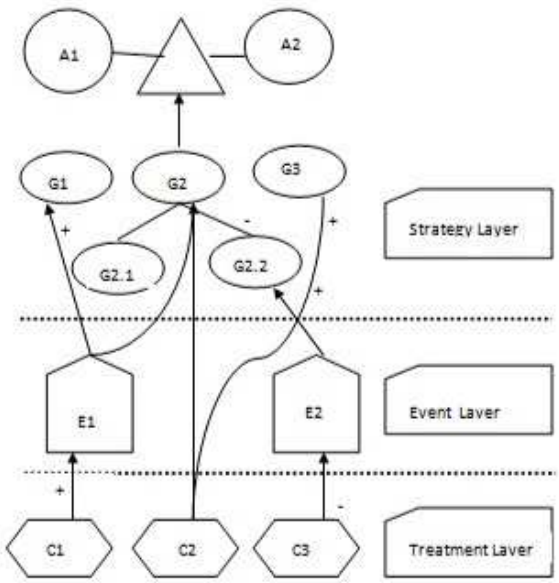

Figure 5-1: Conceptual Layers of the Proposed Framework

while a treatment is a countermeasure that can be adopted in order to mitigate the effects of the risk.

Graphically, an event is presented as a pentagon (the same representation as is used in GR Tropos) and a treatment is depicted as a hexagon. Adopting the idea of the three-layer analysis in GR Tropos, three different layers of goal models are depicted in Figure 5-1.

- **Strategic layer**
  The strategic interests of the stakeholders and action characterization of the goal are modeled in the first layer;
- **Event layer**
  In the second-layer, risks that are relevant to the goal layer are analyzed;
- **Treatment layer**
  In the treatment layer, countermeasures for mitigating risks are introduced.

Below are listed all of the possible relationships between goals, events and treatments.

- **Goal - Event**
  models that a goal increases/reduces the occurrence of an event;
- **Goal - Treatment**
  models that a goal supports/prevents a countermeasure;

- **Event - Goal**
  models risk, namely the impact of an event on goal fulfillment;
- **Event - Treatment**
  models the influence of the occurrence of an event on the countermeasure;
- **Treatment - Goal**
  models the side effects (negative or positive) of a countermeasure on the goal layer;
- **Treatment - Event**
  models the effect of a countermeasure on the mitigation of a risk.

The complete meta-model of the proposed framework is presented in Figure 5-2. This meta-model should be able to represent both legal prescriptions and the intentional model. In this proposed framework, modeling law is the first step of the process, which continues with the modeling of the intentional part as the next step.

The legal part of the meta-model is adopted from NOMOS [4], and consists of six classes, namely *Right*, *Actor*, *ActionCharacterization*, *Dominance*, *Realization*, and *Goal*. There are four sub-classes of the abstract class *Right*, namely *PowerLiability*, *ClaimDuty*, *ImmunityDisability* and *PrivilegeNoclaim*. The subject of *Right* is *Actor*, and it is connected to *Right* by holder and counterparty relation. The concept of *Realization* is representing a goal which fits the characterization given by law. The *Realization* class represents the relation between one element of the legal model and one element of the goal model. Each *Right* is in concerns relations with exactly one *ActionCharacterization*, but one *ActionCharacterization* can be addressed by a number of rights. The *Goal* class will be discussed as part of the intentional meta-model. The last class in the legal part is *Dominance* class which represents a link between two prescribed actions and is labelled with a ">" symbol that goes from the dominant action to the dominated one.

In the intentional meta-model, goals, events and treatments can be decomposed into sub-goals, sub-events and sub-treatments, which are related through contribution relations to other goals, events, and treatments. Moreover, intra-layer and inter-layer relations are adopted in full from GR Tropos in order to capture all possible situations. Each goal has two attributes: SAT and DEN, which quantify the value of evidence and can be divided into the range of $(F)ull, (P)artial, (N)one$. An event becomes a risk when it produces a negative effect, whereas it is an opportunity if it produces a positive effects. An event is characterized by two properties: likelihood and severity/impact. Likelihood is defined as how likely an event is to occur, while impact is the influence of an event on goal fulfillment. Similarly to goals and events, a treatment also has SAT and DEN to represent the evidence that supports and prevents the action. A treatment has an effect on the event layer, and particularly on risks. The effect of the treatment is represented as a relationship, and its value is expressed by the sign of the contribution relationship. There are four types of contribution relations: $+$,$++$,$-$, and $--$. AND/OR decomposition relations are used to refine goals, events, and treatments in order to produce a finer structure.

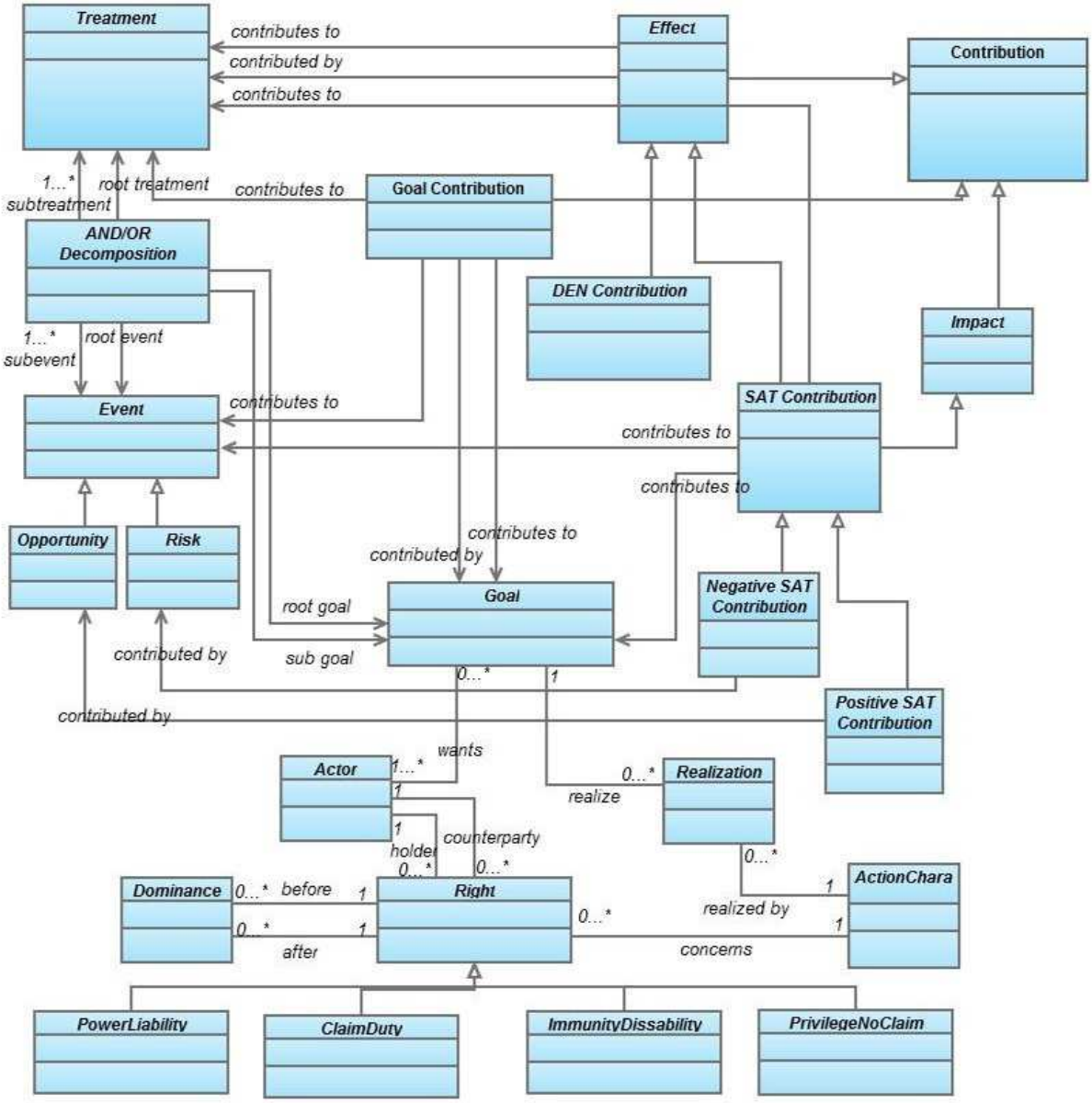

Figure 5-2: Meta-model of the Proposed Framework

5-2 Legal Risk Analysis

This section will present the method for performing the risk reasoning process of legal risk analysis, as seen in Figure 5-3. Two steps are taken to calculate a legal risk analysis with the proposed framework, which are the legal risk reasoning process (A) and the law propagation process (B). The legal risk reasoning process is performed using Algorithm 2, which will be discussed in subsection 5.2.1. In subsection 5.2.2, the law propagation process will also be explained in detail.

For the legal risk reasoning process, three sub-processes are performed. The first process is to assign NPs to each actor (A.1). The second sub-process is the risk reasoning process (A.2) which is performed using Algorithm 1, as discussed in the previous chapter. The last sub-process involves checking the compliance of the requirements with the law (A.3).

5-3 Legal Risk Reasoning

The proposed framework that integrates NOMOS and GR Tropos has been delevoped in order to capture both the law model and the intentional model. Given a normative proposition NP that specifies an action A_{NP}, a goal G is searched for the addressed actor, such that:

- The actor is known to have, the ability to achieve the goal, taking into account events and treatments that have an impact on the goals.
- There is at least one goal which fulfills the NP;

By modifying NOMOS' algorithm [4], the process sketched in Algorithm 2 aims to support the analyst in verifying the compliance of a GR Tropos goal model is performed.

Initially, input from both the GR Tropos goal model and the law model is taken in line 1. Subsequently, in lines 2-4, the rights of each actor in the GR Tropos model are assigned according to the law model. Then, in line 5-6, the NPs of each actor are evaluated. In line 7, the model tries to find at least one goal from the actors' goals that realizes the action specified by the NP. In line 10, if there is a goal that realizes the NP, it is added to the set of assumptions. In lines 11-20, if the goal is decomposed, then its sub-goals have to be analyzed as well as all incoming contributions, delegations, events and treatment. The process in lines 11-20 is calculated using Algorithm 1 from the paper [2], that was discussed in the previous chapter. This process verifies whether or not there is a goal that prevents G from realizing NP.

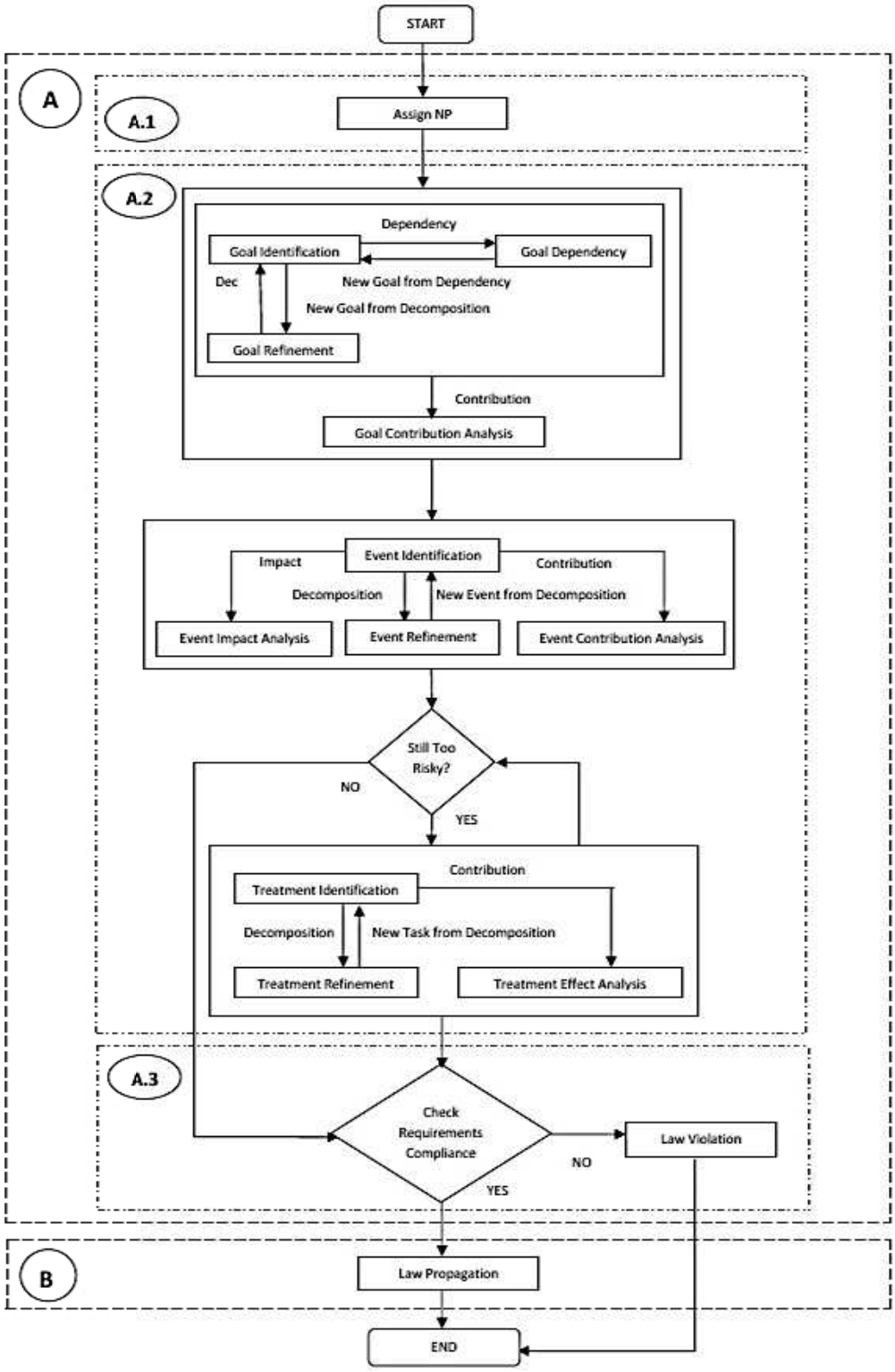

Figure 5-3: Overall Legal Risk Analysis Process

Alg. 2 A sketch of the algorithm - Integration of GRModel and LawModel

```
1: Input : GRModel, LawModel
2: foreach Actor j [addressed by] LawModel do
3:    [Assign rights to j];
4: end
5: foreach Actor j do
6:   foreach NormativeProposition NP ∈ j do
7:     foreach Goal G ∈ j do
8:         try
9:           if G realises A_NP then
10:             [Add 'realization(G, A_NP)' to assumptions];
11:             foreach [goal in G's decomposition] do
12:                 [Analyse decompositions of G];
13:             foreach [contributing goal] do
14:                 [Analyse contribution of G];
15:             foreach [delegated goal] do
16:                 [Analyse delegations of G];
17:             foreach [event] do
18:                 [Analyse event of G];
19:             foreach [treatment] do
20:                 [Analyse treatment of G];
21:         or
22:           [remove G from assumptions];
23:           if hasToComply(j, NP) then
24:             [Throw violation for NP];
25:     end
26:   end
27: end
```

If no goals exist that can realize NP, the assumption that the G can realize the NP has to be removed, as described in line 22. Finally, in lines 23-24, if no suitable goal exists in the set of assumptions and if the NP requires a realization, then a violation occurs and the algorithm determines the non-compliance of the GR model.

5-4 Law Propagation

By adopting the ideas contained in NOMOS [4] regarding the legal concept, the legal risk reasoning described in this section was developed. NOMOS introduces the concept of intentional compliance, i.e., if every actor fulfils its goals, then the law is being respected.

However, an actor might not be capable of fulfilling his/her goals and tasks. An actor may delegate the fulfillment of a goal to other actors. In general, delegation is used to model the transfer of responsibilities from one actor (the delegator) to another (the delegatee). This idea could be used to model law propagation when rights are delegated to another actor. Based on the Hohfeldian concept of rights, law propagation model can be divided into two types, namely:

- **Transferable Rights**

  This means that if an actor passes a right to the counterparty, then the counterparty automatically has the right to pass the right on to another actor. In other words, the law of transitivity holds for transferable rights. The rights that are considered to be transferable rights are $Power$ and $Privilege$.

$$Transferable(j, NP) = NP(j_a, j_b, A) \tag{5-1}$$

  where Power, Privilege $\in NP$, and A is an Action.

$$PowerLiability(j_a, j_b, delegate(j_a, j_b, A)) \rightarrow PowerLiability(j_b, j_c, A) \tag{5-2}$$

$$PrivilegeNoClaim(j_a, j_b, delegate(j_a, j_b, A)) \rightarrow PrivilegeNoClaim(j_b, j_c, A) \tag{5-3}$$

  The concept of transferable rights means that when an actor is assigned these rights (i.e., $Power$ and $Privilege$), then this actor is capable of delegating them to another actor. For example, if one has the power to enter a building using a smartcard, then one has power to give this card to anyone so that they may enter the building.

- **Non Transferable Rights**

  Contrarily, non-transferable rights mean that if an actor delegates a right, the counterparty cannot pass this right to another actor. *Duty* and *Disability* belong to the category of non-transferable rights.

$$NonTransferable(j, NP) = NP(j_a, j_b, A) \tag{5-4}$$

  where Duty, Disability $\in NP$, and A is an Action.

$$ClaimDuty(j_a, j_b, delegate(j_a, j_b, A)) \rightarrow ClaimDuty(j_a, j_b, A) \tag{5-5}$$

$$ImmunityDissability(j_a, j_b, delegate(j_a, j_b, A)) \rightarrow ImmunityDissability(j_a, j_b, A). \tag{5-6}$$

  The concept of non-transferable rights means that when an actor is assigned these rights (i.e., *Duty* and *Disability*), then this actor has an obligation to use them. For example, if a student is claimed by his professor to have a duty to do his homework, then he has to do it by himself and cannot delegate this duty to finish his homework to his friend.

Taken from NOMOS [4], the legal risk analysis process above is equipped with a set of rules for compliance with the law, as follows.

Rule 1. Ability
If an action has to be realized by an actor, then the actor must have at least one goal that realizes the action. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

Rule 2. Decomposition
If a goal G represents the ability of an actor to realize a certain NP, then for each sub-goal of G, by achieving that sub-goal, the NP must still be realized. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

Rule 3. Contribution
If a goal G represents the ability of an actor to realize a certain NP and the goal is the target of a contribution, then by achieving the contribution of the source goal, the NP must still be realized. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

Rule 4. Delegation
If a goal is (a part of) the ability of an actor to realize a certain NP and it is delegated

to another actor, then Rule 2 must hold for the delegatee. The achievement of the goal(s) involves taking an acceptable level of risk into consideration.

Rule 5. Duty
If a N is a duty which specifies that an action must be performed by a specific actor, then the action must be realized by the actor.

Rule 6. Privilege, Claim and Power
If an actor has a claim, then the actor can discretionally decide to realize the claim through the use of an ability. Note that these rights are different from each other for the counterparties, but as they are only somewhat different for the holders, we will not draw such distinctions here.

Rule 7. Liability and Immunity
If an actor experiences a liability, such as a sanction, it may want to prevent the sanction from being applied by searching for immunity. In this case, realizing this immunity overcomes the liability.

Rule 8. No-claims and Disability
If an actor experiences a no-claim or a disability, then the action cannot be realized.

Chapter 6

Evaluation

In this chapter, the proposed framework from Chapter 5 will be implemented and evaluated using the scenario described in Chapter 2. Using the graphical notation of the proposed framework, the scenario will be modeled in section 6.1. The legal risk analysis process which was performed in order to evaluate compliance with the law in the scenario will be presented in section 6.2.

6-1 Scenarios applied to the Proposed Framework

The scenario in Chapter 2 will be modeled using the proposed framework with its graphical notation and features as depicted in Figure 6-1. The legal reference of the model for traceability can be seen in Table 6-1. The proposed framework represents actors as circles, goals as rounded rectangles, events as pentagons and treatments as hexagons. It is also equipped with a symbol for law modeling, which is depicted as a rectangle.

In Scenario 1, when Patients share their PHR info with the PHR Provider, they assign a Claim Duty to the PHR Provider. Moreover, once Patients share their PHR Info, they are also granted three rights (i.e., the right to be informed, the right to access and the right to object), based on the Directive. These rights are captured using Power Liability rights. Patients share their info with the PHR Provider in order to fulfill their goal to Get Medical Services. This goal can be decomposed into three sub-goals, namely Get Medical Treatment, Get Medical Insurance and Provide PHR Info. The fulfillment of the goal to Provide PHR Info is affected by the risk that is represented as an event that may occur. In this case, the risk that data may be misused obstructs the fulfillment of the goal to Provide PHR info, and it has a negative impact on the goal. One of the ways to mitigate the risk is by introducing a treatment. The Privacy Policy treatment is used in this case so that the Patients' medical information will not be misused. The Privacy Policy treatment

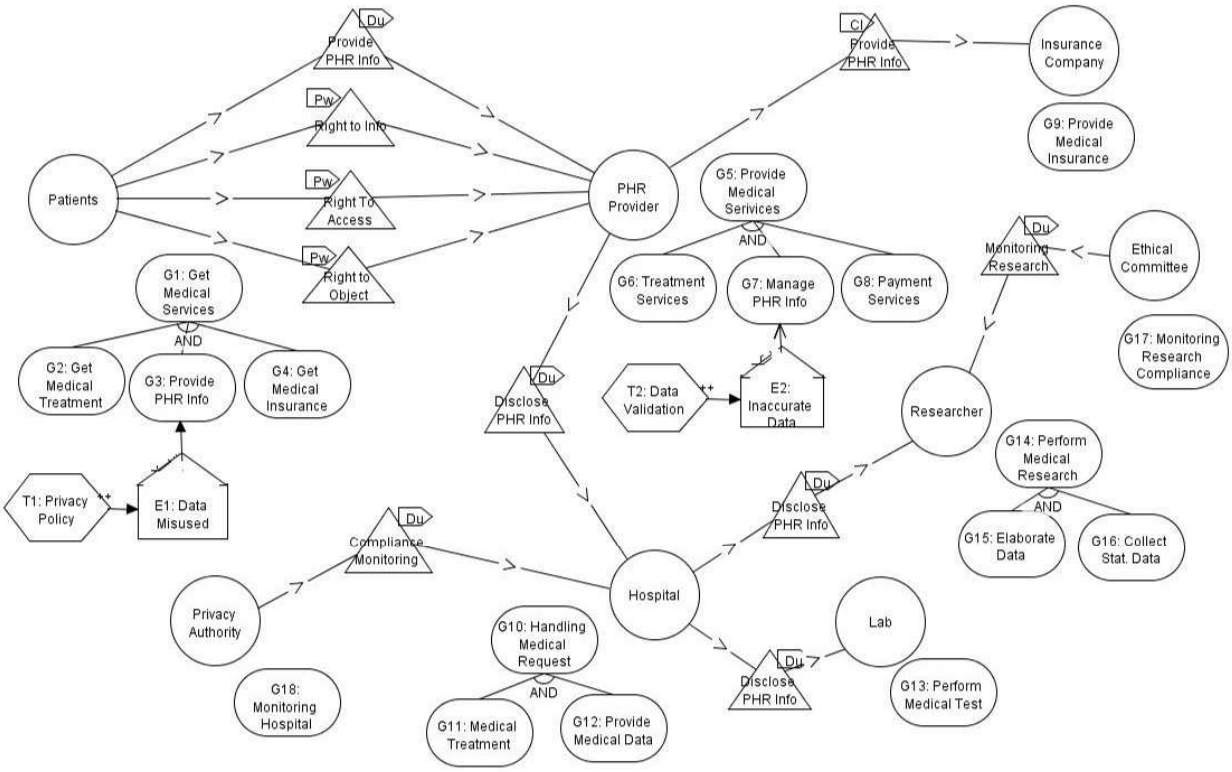

Figure 6-1: Proposed Framework Model

Table 6-1: Law Reference

Src	Id	Right	Holder	Cp	Action
Article 6	NP1	CD	Patients	PHR Provider	Provide PHR Info
Article 10	NP2	PL	Patients	PHR Provider	Right to Info
Article 12	NP3	PL	Patients	PHR Provider	Right to Access
Article 14	NP4	PL	Patients	PHR Provider	Right to Object
Article 6	NP5	CD	PHR Provider	Insurance Company	Disclose PHR Info
Article 6	NP6	CD	PHR Provider	Hospital	Disclose PHR Info
Article 6	NP7	CD	Hospital	Lab	Disclose PHR Info
Article 6	NP8	CD	Hospital	Researcher	Disclose PHR Info
Article 31	NP9	CD	Ethical Committee	Researcher	Compliance Monitoring
Article 28	NP10	CD	Privacy Authority	Hospital	Compliance Monitoring

is introduced so that Patients will know beforehand the purpose for which their data are being used, as prescribed in the Privacy Policy.

With regard to Scenario 2, the PHR Provider has a goal, namely to Provide Medical Services, that can be decomposed into three sub-goals, which are Manage PHR Info, Treatment Service and Payment Service. The information that is managed by the PHR Provider has to be accurate, as the information will be shared with the other actors who need it. The goal of Manage PHR Info carries a risk, which is that the data might be inaccurate. This risk is mitigated by implementing a Data Validation treatment. For example, if Patients need help with managing their insurance, then the PHR Provider will share the patients' personal information with the appointed Insurance Company. This is captured with the Claim Duty through which the PHR Provider discloses PHR Info to the Insurance Company.

As in Scenarios 3 and 4, the PHR Provider also has a duty to disclose the Patient's medical information to the Hospital. In this scenario, the PHR Provider discloses the information to the Hospital so that the Hospital can provide any kind of service to the Patient. In cases in which Patients need medical tests, the Hospital will disclose the Patients' medical information to the Lab, which is captured with a Claim Duty right.

The Hospital also has the goal of Handling Medical Requests, which can be decomposed into two sub-goals, namely Medical Treatment and Provide Medical Data. The goal of Provide Medical Data deals with the Hospital's duty to disclose Patients' medical information to the Researcher for research purposes, as discussed in Scenario 5.

Scenario 6 and Scenario 7 deal with the duty of Ethics Committee to monitor the Researcher and also the duty of the Privacy Authority to monitor the compliance of the Hospital.

From the model, it is clear that the proposed framework is able to model both the law and intentional models.

6-2 Legal Risk Analysis

In order to apply legal risk analysis to the scenario using the proposed framework, the process outlined in Figure 5-3 is performed. Using the model depicted in Figure 6-1, each actor is evaluated.

6-2-1 Patients

The legal risk reasoning process (Process A) is performed using Algorithm 2. The first step (A.1) involves assigning $NP1$, $NP2$, $NP3$ and $NP4$ to Patients.

The next step (A.2) starts with taking as input the extended goal model and a set of desired values for top goals (i.e., SAT and DEN), and a number of goals as possible candidates

for the final solution (input goals) that hold for every NP (line 1 of Algorithm 1). For example, G_1 (Get Medical Service) is set to be fully satisfied G_1 ($Sat(G_1) = F$) without any risk ($Den(G_1) = N$). This value is set, as Patients want their goal of Getting Medical Treatment to be fully satisfied without being afraid that their PHR Info will be misused.

Backward_Reasoning (line 2 of Algorithm 1) generates a set of possible assignment values for the input goals that can satisfy the desired values. In order to fully satisfy G_1, the only alternative solution is $\{G_2, G_3, G_4\}$ which is called *candidate_solution* (line 3 of Algorithm 1).

The *candidate_solution* is now evaluated against risks and then necessary countermeasures are introduced (lines 4-18 of Algorithm 1). First, it is checked whether the *candidate_solution* needs countermeasures in order to obtain the desired values in the top goals. As there is an associated risk (Data Misused), a countermeasure is introduced (Privacy Policy).

In order to define the countermeasures, the maximum assignable risk values that produce an acceptable DEN value for the top goal must be found. In this scenario, $Den(G_1 = N)$ is set. Then, line 9 of Algorithm 1, $Standard\_Forward\_Reasoning$ is used to propagate the input values of the candidate solution in the model and to evaluate the impact of the risk. Using $Calc\_Event$, the acceptable values for the event (i.e., values that can still satisfy the desired top goals) can be calculated, which produce $Den(E_1) = P$ (line 10 of Algorithm 1).

In line 11 of Algorithm 1, *Backward_Reasoning* is once again applied in order to find possible treatments that can guarantee an acceptable level of risk. The only possible treatment in the model is T_1.

The impact of E_1 on the goal G_1 depends on the SAT value. The effect of T_1 on G_1 is to increase the $Den(E_1) = P$. A countermeasure is effective when it is able to generate a conflict between SAT and DEN of the risk .

As the desired risk value for G_1 is $Den(G_1 = N)$, but E_1 produces a partial denial which is $Den(E_1) = P$, countermeasures are introduced in order to create a conflict so that E_1 does not have an impact on G_1. In this case, $Calc\_Event$ will produce acceptable risk values $Den(E_1) = P$ in order to neutralize the $Sat(E_1) = P$ (line 10 of Algorithm 1).

As the input goal can satisfy the top goal, based on the concept of Intentional Compliance, then the law is respected, with the value of the top goal is ($Sat(G_1) = F, Den(G_1) = N$) and the value of acceptable risk is ($Sat(E_1) = P, Den(E_1) = P$) (the last step, A.3).

With regard to the law propagation process (Process B), the NP of patients is propagated based on the type of rights, as explained in the previous section. As $NP1$ is Claim Duty, this right cannot be transferred, which means that the duty of providing PHR Info has to be carried out by the Patients themselves. However, for the other NPs ($NP2$, $NP3$, and $NP4$), which are Power Liability, these rights can be transferred, which means that the counterparty (i.e., the PHR Provider) also has the power to check patients' data when

it is given to the PHR Provider's counterparties (i.e., the Insurance Company and the Hospital).

6-2-2 PHR Provider

For the second actor, the legal risk analysis is performed in the same manner as for Patients. In the legal risk analysis process (Process A), the first step (A.1) is to assign the PHR Provider with $NP5$ and $NP6$.

The process of legal risk reasoning (A.2) is performed based on Algorithm 1 [2]. The first step is to set the desired values for the top goal G_5 (i.e., Provide Medical Services) with fully satisfy, ($Sat(G_5) = F$) without any risk ($Den(G_5) = N$), and taking a number of goals as possible candidates (line 1 of Algorithm 1). This value is set, as the PHR Provider wants the received PHR Info to be accurate when providing medical services.

In order to fully satisfy G_5, the only *alternative_solution* is $\{G_6, G_7, G_8\}$, and it is considered to be *candidate_solution*. As there is a risk (Inaccurate Data) associated with them, a countermeasure (Data Validation) is introduced. In order to define the countermeasures, the maximum assignable risk values that produce an acceptable DEN value for the top goal have to be found, and in this scenario $Den(G_5 = N)$ is set. Then, in line 9 of Algorithm 1, $Standard\_Forward\_Reasoning$ is used to propagate the input values of the candidate solution in the model and to evaluate the impact of the risk. By using $Calc\_Event$ in line 10 of Algorithm 1, the acceptable values for the event (i.e., values that can still satisfy the desired top goals) can be calculated, which produce $Den(E_2) = F$.

In line 11 of Algorithm 1, *Backward_reasoning* is once again applied to find possible treatments that can guarantee acceptable levels of risk. The only possible treatment in the model is T_2.

The impact of E_2 on the goal G_5 depends on the SAT value. The effect of T_2 on G_5 is to increase the $Den(E_2) = F$. A countermeasure is effective when it is able to generate a conflict between SAT and DEN of the risk.

As the desired risk value for G_5 is $Den(G_5 = N)$, but E_2 produce $Den(E_2) = F$, therefore countermeasures are introduced in order to create a conflict so that E_2 does not have an impact on G_5. In this case, $Calc\_Event$ produces acceptable risk values $Den(E_2) = F$ in order to neutralize the $Sat(E_2) = F$ (line 10 of Algorithm 1).

As the input goal can satisfy the top goal, based on the concept of intentional compliance, then the law is respected, with the value of the top goal is $(Sat(G_5) = F, Den(G_5) = N)$ and the value of acceptable risk is $(Sat(E_2) = F, Den(E_2) = F)$ (the last step, A.3).

With regard to the law propagation process (Process B), the NP of the PHR Provider is Claim Duty. Based on the type of rights, as explained in the previous section, this right is non-transferable, which means that the duty that is claimed by the PHR Provider cannot be transferred to any of its counterparties (i.e., the Insurance Company and the Hospital).

6-2-3 Hospital

The legal risk analysis process is also used to evaluate the third actor, which is the Hospital. Process A is performed using Algorithm 2. The first step of process A (A.1) assigns $NP7$ and $NP8$ to the Hospital. The second step (A.2) involves performing legal risk reasoning using Algorithm 1 to calculate acceptable risk values so that the input goals can satisfy G_{10} (i.e., Handling Medical Request).

The first step is to set the desired values for goal G_{10}, fully satisfying ($Sat(G_{10}) = F$) without any risk ($Den(G_{10}) = N$) and a taking number of goals G_{11} and G_{12} into consideration as possible candidates.

In order to fully satisfy G_{10}, the only alternative solution is $\{G_{11}, G_{12}\}$, which is called the candidate solution (line 3 of Algorithm 1). The candidate solution is now evaluated against risks. As there are no risks that are associated with them, they are considered as a solution. This means that the top goal is satisfied, based on the concept of intentional compliance, then the law is respected, with the value of the top goal is ($Sat(G_{10}) = F, Den(G_{10}) = N$) (the last step, A.3).

The law propagation process (Process B) is performed by checking the NP of the Hospital. Both of the Hospital's NPs are Claim Duty, which are considered to be non-transferable rights. Therefore, the duty that is assigned to the Hospital has to be carried out by the Hospital and cannot be transferred to any of its counterparties (i.e., Researchers or the Lab).

6-2-4 Ethics Committee

For the fourth actor, the legal risk analysis is performed in the same manner as for the other actors. With regard to process A, the first step (A.1) involves the Ethics Committee being assigned $NP9$. The process of legal risk reasoning (A.2) is performed based on Algorithm 1 [2]. As stated in the compliance rule regarding ability, if an action has to be realized by an actor, then the actor must have at least one goal that realizes the action. As there is only one goal that has to be achieved by the Ethics Committee (i.e., Monitoring Research Compliance), the model is compliant.

In order to perform the law propagation process (Process B), the NP of the actor is checked based on the type of rights. The NP of the Ethics Committee is Claim Duty, which is considered to be a non-transferable right, and therefore the duty of Monitoring Research Compliance has to be performed by the Ethics Committee and cannot be performed by any of its counterparties.

6-2-5 Privacy Authority

The legal risk analysis process is also used to evaluate the fifth actor, which is the Privacy Authority. Process A is performed using Algorithm 2. The first step in process A, which

is A.1, assigns $NP10$ to the Privacy Authority. The second step (A.2) involves performing legal risk reasoning using Algorithm 1. The Privacy Authority has only one goal, and therefore the model is compliant based on the rule of compliance regarding ability.

The law propagation process (Process B) is performed by checking the NP of the Privacy Authority. The Privacy Authority's NP is Claim Duty, which is considered to be a non-transferable right. Therefore, the duty of Monitoring Hospital Compliance that is assigned to the Privacy Authority has to be done by the Privacy Authority and cannot be transferred to any of its counterparties (i.e., the Hospital). In other words, the duty of the Privacy Authority in monitoring the Hospital cannot be performed by the Hospital, because if this was the case, then the Hospital might violate the law, as it would be the Hospital itself which would be monitoring compliance.

Chapter 7

Conclusions

7-1 Conclusions

The problems associated with modeling and analyzing the law with the purpose of establishing the compliance of an IT system with legal requirements in risk analysis using certain frameworks have been studied in this thesis. Some frameworks have already been proposed, such as CORAS and GR Tropos for modeling risk analysis, and Extended CORAS and NOMOS for modeling legal analysis.

The NOMOS framework is a modeling language that supports the representation of intentional and normative elements. Unfortunately, NOMOS does not consider risks which occur during the requirements analysis, therefore it is not possible to analyze the effects of unpredictable situations on stakeholders' goals. The GR Tropos framework is used to model and to reason risk within the requirements engineering process, but it cannot capture the legal aspect of a scenario.

In this thesis, a framework for assessing legal risk was developed by integrating NOMOS and GR Tropos. NOMOS was used as the basis for law modeling, as it has features which can capture laws in full, while GR Tropos was used as the basis for risk modeling, as it is equipped with treatments and events. Moreover, the integration of NOMOS and GR Tropos is very easy to do, as both of them are goal-oriented frameworks.

The first contribution of this work is the meta-model of the proposed framework. The law meta-model was adapted from NOMOS, while the intentional meta-model was taken from GR Tropos, which resulted in the graphical notation for modeling a scenario and capturing both the law model and the intentional model. The second contribution is the introduction of the three-layer model of the proposed framework, in which risks are related to goals and countermeasures by incorporating the new primitive event and treatment. The new constructs were formalized so that the risk of a system could be analyzed in a legal

framework. The third contribution is the introduction of the notion of law propagation, which consists of transferable and non-transferable rights. The proposed framework has been applied and evaluated by assessing the legal risk of a healthcare service. Based on this evaluation result, it shows that the proposed framework is able to model both the law model and the intentional model.

7-2 Future Work

In order to utilize a framework to its full potential, it has to be understandable, as security risk analysis techniques involve people from different backgrounds. Therefore, in the future, this proposed framework, which integrates GR Tropos and NOMOS, should be developed with a graphical approach like that of CORAS, a framework that supports the security analysis process. This idea is based on the results of section 4.3. A more user-friendly graphical approach will reduce misunderstandings and provide a more correct picture of risk.

TEST PAGE: References Link for the thesis: [3] [3] [5] [4] [2] [10] [11] [12] [14] [15] [17] [16] [18] [19] [26] [20] [21] [25] [27] [28] [29] [30] [31] [32] [33] [34] [35] [23] [36] [37] [38] [39] [40] [41] [6] [7] [9] [1] [22] [42] [43]

Bibliography

[1] R. Fredriksen, M. Kristiansen, B. A. Gran, K. Stølen, T. A. Opperud, and T. Dimitrakos, "The coras framework for a model-based risk management process," in *SAFECOMP*, ser. Lecture Notes in Computer Science, S. Anderson, S. Bologna, and M. Felici, Eds., vol. 2434. Springer, 2002, pp. 94–105.

[2] Y. Asnar, P. Giorgini, and J. Mylopoulos, "Risk modelling and reasoning in goal models," *Technical Report DIT-06-008, University of Trento*, 2006.

[3] F. Vraalsen, M. S. Lund, T. Mahler, X. Parent, and K. Stølen, "Specifying legal risk scenarios using the coras threat modelling language," in *iTrust*, ser. Lecture Notes in Computer Science, P. Herrmann, V. Issarny, and S. Shiu, Eds., vol. 3477. Springer, 2005, pp. 45–60.

[4] A. Siena, J. Mylopoulos, A. Perini, and A. Susi, "The nomos framework: Modelling requirements compliant with laws," *Technical Report TR-0209-SMSP, FBK - Irst*, 2009.

[5] M. Kim and K. Johnson, "Personal health records: evaluation of functionality and utility," *J Am Med Inform Assoc. 9 (2)*, pp. 171–180, 2002.

[6] Google, "Google health - http://www.google.com/intl/en-us/health/about/devpp.html," 2011.

[7] Microsoft, "Microsoft health vault - http://www.healthvault.com/personal/index.aspx," 2011.

[8] M. M. M. P. D., "The mental health professional and the new technologies: A handbook for practice today," 2005.

[9] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, European Commission, 1995.

[10] ISO/IEC, "Risk management vocabulary guidelines for use in standards," *ISO/IEC Guide 73*, 2002.

[11] DoD, "Military standard, procedures for performing a failure mode, effects, and critical analysis," *MIL-STD-1629A*, 1980.

[12] ISO, "Hazard and operability studies (hazop studies) - application guide," *IEC61882*, 2001.

[13] D. o. P. NSW Goverment, "Hazardous industry planning- advisory paper no 8 : Hazop guidelines," 2008.

[14] T. Bedford and R. Cooke, "Probabilistic risk analysis: Foundations and methods," *Cambridge University Press*, 2001.

[15] S. Butler and P. Fischbeck, "Pmulti-attribute risk assessment," *Technical Report CMU-CS-01-169*, 2001.

[16] I. Guide, "Fault tree analysis (fta)," *IEC61025*, 1990.

[17] ——, "Analysis techniques for system reliability - procedures for failure mode and effect analysis (fmea and fmeca)," *IEC60812*, 1985.

[18] C. Biagioli, P. Mariani, and D. Tiscornia, "Esplex: A rule and conceptual based model for representing statutes," *Proc. of the 1st.*

[19] L. L.E. Allen, "Symbolic logic: A razor-edged tool for drafting and interpreting legal documents," *Yale Law Journal 66(6)*, pp. 833–879, May 1957.

[20] J. Meyer and R. Wieringa, "Deontic logic in computer science: normative system specification," *Wiley, NY*, May 1994.

[21] W. Hofeld, "Fundamental legal conceptions as applied to judicial reasoning," *Yale Law Journal*, pp. 16–59, May 1913.

[22] E. Yu, "Modelling strategic relationships for process engineering," *PhD thesis, University of Toronto, Department of Computer Science*, 1995.

[23] P. Giorgini, J. Mylopoulos, and R. Sebastiani, "Goal-oriented requirements analysis and reasoning in the tropos methodology," *Eng. Appl. of AI*, vol. 18, no. 2, pp. 159–171, 2005.

[24] Y. Asnar, R. Moretti, M. Sebastianis, and N. Zannone, "Risk as dependability metrics for the evaluation of business solutions: A model-driven approach," in *ARES*. IEEE Computer Society, 2008, pp. 1240–1247.

[25] F. Vraalsen, F. den Braber, M. S. Lund, and K. Stølen, "The coras tool for security risk analysis," in *iTrust*, ser. Lecture Notes in Computer Science, P. Herrmann, V. Issarny, and S. Shiu, Eds., vol. 3477. Springer, 2005, pp. 402–405.

[26] L. Compagna, P. E. Khoury, F. Massacci, R. Thomas, and N. Zannone, "How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach," in *ICAIL*. ACM, 2007, pp. 149–153.

[27] M. S. Feather, S. L. Cornford, K. A. Hicks, and K. R. Johnson, "Applicatiuons of tool support for risk-informed requirements reasoning," *Comput. Syst. Sci. Eng.*, vol. 20, no. 1, 2005.

[28] Y. Asnar, P. Giorgini, R. Bonato, V. Meduri, and C. Riccucci, "Secure and dependable patterns in organizations: An empirical approach," in *RE*. IEEE, 2007, pp. 287–292.

[29] T. J. M. Bench-Capon, "Support for policy makers: Formulating legislation with the aid of logical models," in *ICAIL*, 1987, pp. 181–189.

[30] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, and J. Mylopoulos, "Tropos: An agent-oriented software development methodology," *Autonomous Agents and Multi-Agent Systems*, vol. 8, no. 3, pp. 203–236, 2004.

[31] S. A. Butler, "Security attribute evaluation method: a cost-benefit approach," in *ICSE*. ACM, 2002, pp. 232–240.

[32] F. den Braber, T. Dimitrakos, B. A. Gran, M. S. Lund, K. Stolen, and J. A. Aagedal, "The coras methodology: Model-based risk assessment using uml and up," *In UML and the Unified Process Idea Group*, pp. 332–357, May 2003.

[33] F. den Braber, A. B. Mildal, J. Nes, K. Stølen, and F. Vraalsen, "Experiences from using the coras methodology to analyze a web application," *J. Cases on Inf. Techn.*, vol. 7, no. 3, pp. 110–130, 2005.

[34] H. E. I. Dahl, I. Hogganvik, and K. Stolen, "Structured semantics for the coras security risk modelling language," *In Pre-proceedings of the 2nd International Workshop on Interoperability solutions on Trust, Security, Policies and QoS for Enhanced Enterprise Systems (IS-TSPQ'07) - Department of Computer Science, University of Helsinki*, pp. 79–92, May 2007.

[35] S. Ghanavati, D. Amyot, and L. Peyton, "Towards a framework for tracking legal compliance in healthcare," in *CAiSE*, ser. Lecture Notes in Computer Science, J. Krogstie, A. L. Opdahl, and G. Sindre, Eds., vol. 4495. Springer, 2007, pp. 218–232.

[36] P. Giorgini, F. Massacci, and N. Zannone, "Security and trust requirements engineering," in *FOSAD*, ser. Lecture Notes in Computer Science, A. Aldini, R. Gorrieri, and F. Martinelli, Eds., vol. 3655. Springer, 2005, pp. 237–272.

[37] P. Guarda and N. Zannone, "Towards the development of privacy-aware systems," *Information & Software Technology*, vol. 51, no. 2, pp. 337–350, 2009.

[38] I. Hogganvik and K. Stølen, "A graphical approach to risk identification, motivated by empirical investigations," in *MoDELS*, ser. Lecture Notes in Computer Science, O. Nierstrasz, J. Whittle, D. Harel, and G. Reggio, Eds., vol. 4199. Springer, 2006, pp. 574–588.

[39] A. Siena, J. Mylopoulos, A. Perini, and A. Susi, "From laws to requirements," *1st International Workshop on Requirements Engineering and Law (Relaw'08) Barcelona, Spain*, May 2008.

[40] A. Siena, "Engineering normative requirements," in *RCIS*, C. Rolland, O. Pastor, and J.-L. Cavarero, Eds., 2007, pp. 439–444.

[41] ISO/IEC, "Standardization and related activities - general vocabulary," *ISO/IEC Guide 2*, 2004.

[42] P. Giorgini, J. Mylopoulos, E. Nicchiarelli, and R. Sebastiani, "Formal reasoning techniques for goal models," *J. Data Semantics*, vol. 1, pp. 1–20, 2003.

[43] R. Sebastiani, P. Giorgini, and J. Mylopoulos, "Simple and minimum-cost satisfiability for goal models," in *CAiSE*, ser. Lecture Notes in Computer Science, A. Persson and J. Stirna, Eds., vol. 3084. Springer, 2004, pp. 20–35.

[44] P. Herrmann, V. Issarny, and S. Shiu, Eds., *Trust Management, Third International Conference, iTrust 2005, Paris, France, May 23-26, 2005, Proceedings*, ser. Lecture Notes in Computer Science, vol. 3477. Springer, 2005.