Methodology
of
Security and Dependability using SI*

Contents

Chapter 1

Security and Dependability Tropos

1.1 Security and Dependability Tropos

Security and Dependability Tropos is a formal framework for modeling and analyzing security requirements of an organization. Methodology of Security and Dependability Tropos includes the description of the systematic method to model an organization considering the security, trust and privacy aspects. The methodology is composed of seven phases shown in figure 1.1:

- Actor Modeling - This phase focuses on identifying the stakeholders in the organization. Actor modeling refers to the identification of entities and analysis of hierarchical concept of subordination of entities within the organization.
- Goal Modeling / Functional Modeling - This modeling phase focuses on the identification of strategic interest of the stakeholders in the organization and the dependency among them. This modeling also refines the interests/responsibilities of the entities in the organization into lower level.
- Trust Modeling - It depicts the approach for modeling trust relations between actors in the organizational setting. Trust modeling consists of identifying actors who trust other actors for goal, plans, and resources.
- Process Mapping - This modeling deals with the means-end analysis which aims at identifying plans, resources and soft-goals that provide means for

achieving other goals, executing other plans and producing other resources.

- Permission Mapping - This modeling phase represents the modeling of formal transfer of objectives and authorization from one actor to other. Particularly, this phase deals with the formal passage of rights of a goal or a plan or a resource.

- Side Effect Modeling- This modeling focuses on analyzing the side-effects of the success/failure of business objects (i.e., goals, tasks, resources) on other business objects.

- Risk Modeling - Risk Modeling is the continuous process of systematically identifying, analyzing, treating, and monitoring risk in an organization.

Tips 1.1.1. *The sequence of the methodological phases shown in figure 1.1 is not mandatory to follow. But it is a good practice to follow the sequence described in figure 1.1 for modeling an organization considering the security, trust and privacy aspects.*

1.2 Organization of the Document

This document includes eight chapters. An overview of the entire document can be found from the following small description of the chapters:

Chapter 2: Actor Modeling

Describes the definition, constructs and examples of Actor Modeling in Tropos. This chapter includes:

- Definition of Actors.

- Definition of the constructs employed to understand the organization structure and build role specialization hierarchies.

- Examples of Actor Modeling.

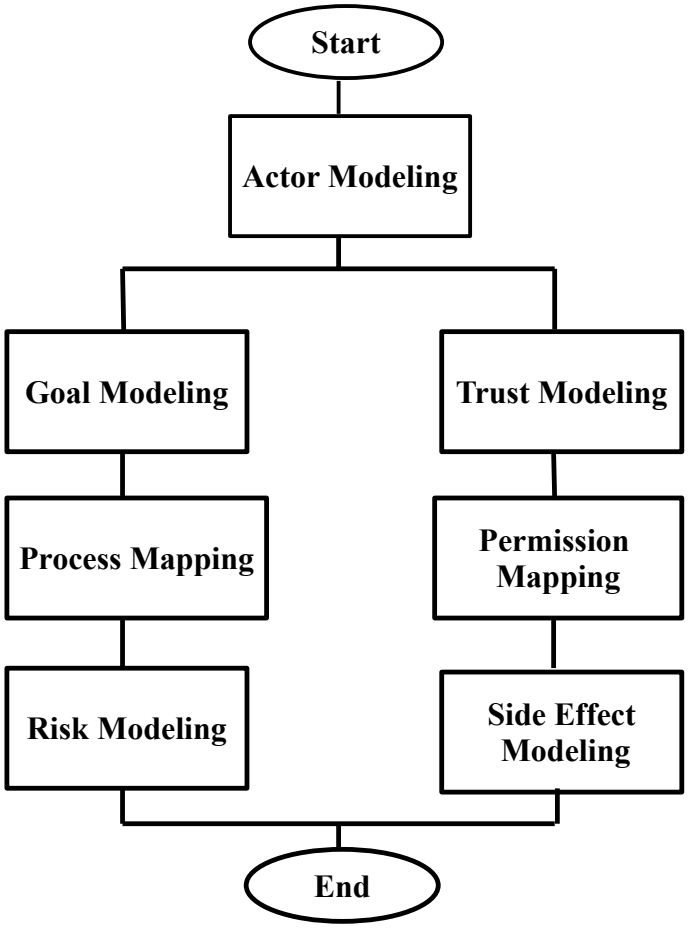

Figure 1.1: Methodological phases of Security and Dependability Tropos

Chapter 3: Goal Modeling

Describes the definition, constructs and examples of Goal Modeling in Tropos. This chapter includes :

- Definition of Goals.
- Definition of the constructs for goal decomposition and dependency.
- Examples of Goal Modeling.

Chapter 4 : Trust Modeling

Describes the definition, constructs and examples of Trust Modeling in Tropos. This chapter includes:

- Definition of Trust and the constructs need for Trust Modeling.
- Defines the process to model the trust environment of an organization.
- Examples of Trust Modeling.

Chapter 5 : Process Mapping

Describes the definition, constructs and examples of Process Mapping in Tropos. This chapter includes:

- Definition of Tasks, Resources, Means-End relation.
- Examples of Process Mapping.

Chapter 6 : Permission Mapping

Describes the constructs of Permission Mapping in Tropos. This chapter includes:

- Concept of Ownership, Provisioning and Requiring of a goal/plan/resource.
- Definition of Delegation Permission.
- Examples of Permission Mapping.

Chapter 7 : Side Effect Modeling

Describes the definition, constructs and examples of Side-Effect Modeling in Tropos. This chapter includes:

- Definition of Contribution Relation.
- Concept of SAT & DEN.
- Steps of Side Effect Modeling.
- Examples of Side Effect Modeling.

Chapter 8 : Risk Modeling

Describes the definition, constructs and examples of Risk Modeling in Tropos.

- Definition of Event and Risk.
- Steps of Risk Modeling which includes Risk Identification and Refinement, Risk Assessment and finally Treatment Analysis.
- Examples of Risk Modeling.

Chapter 9 : Conclusion

This chapter includes the conclusion notes of methodology of Security and Dependability Tropos.

Appendix

For ease of understanding we have used the same organizational scenario as example throughout this document. We have chosen a hospital scenario here, explicitly the Drug Reimbursement process followed by the hospitals. The scenario is defined in sub-section 1.4. Case studies of the Drug Reimbursement scenario for hospitals can be found in Appendix A and B.

- **Appendix A** - This section includes the case study on outpatient Drug Prescription phase followed by the hospitals in the Drug Reimbursement process.
- **Appendix B** - This section includes the case study on report generation and sending phase of Drug Reimbursement process.

1.3 Icons Used in Document

Throughout the book, icons appear in the left margins to mention about special information.

- Examples: The text attached with this icon contains an example of modeling with Tropos.

- Remember: The text attached with this icon includes the idea which can help people to make progress in modeling organization with Tropos.

- Tpis :The text attached with this icon includes a helpful hint for modeling the organization with Tropos.

- Warning : The text attached with this icon includes an information that people need to worry about. It also may include the common mistakes made by people.

- Next Level: The text attached with this icon contains the next level ideas.

1.4 Scenario

This scenario considers the Drug Reimbursement process which is a standard process (called File F) followed by hospitals for being reimbursed the drug distributed among the outpatients. The outpatient drug reimbursement is regulated by the Ministry which provides regulations and guidelines for the hospitals to report about reimbursable drugs. The HealthCare Authority is the responsible organization to supervise hospitals to obey the regulation and guidelines of healthcare services provided by Ministry. Hospital includes Operational Unit where the doctors/nurses are associated with the Operational Unit. The Drug Reimbursement process is composed into four phases:

- **Drug Prescription (P1)** - Prescription phase is executed by the doctors and the patients through the Prescription module of the IT System of the hospital. The process starts when any patient needs the treatment. First the doctor has to identify the patient in order to give a prescription. The patient identification can be done either by patient identification number (e.g., Tax code, STP code, Team code) or the Clinical record. Then doctor retrieves all the past medical record of the patient from the IT System. Then he analyses the past medical reports of the patient and the previous prescribed and dispensed drug list. The doctor selects suitable drugs from the available drug list of the ward stock with which the doctor is associated. Finally he has to register the prescription data. Before the registration confirmation,

the doctor can modify or delete the prescription information. Then the prescription is printed and the doctor has to sign the sheet and give the sheet to the patient. A prescription is the health-care program for the patient which includes the name of the drug items, posology and quantity. Detail description on drug prescription phase is found in Appendix A 9. The prescription phase ends by archiving the prescription of the patient as clinical record to send to the Regional Authority.

- **Drug Dispensation (P2)** - The dispensation phase is conducted by doctors or nurses in the unit where they check the prescription given by doctor and dispense drug from the available drug stock. They also store the dispensed drug information.

- **Generation and Sending of File F report (P3 & P4)** - Generating report and sending it to the Healthcare Authority are the last two phases of Drug Reimbursement process. The Accounting Office of the hospital generates the Drug Reimbursement reports for the Healthcare Authority from the Drug Prescription and Drug Dispensation information. The Administrative Officer of the Accounting Office retrieves and extracts the Drug Prescription and Drug Dispensation information of the hospital using the Hospital IT system and generates the Drug Reimbursement report following the Healthcare regulations. The reports are sent to the Healthcare Authority through the common e-mail systems for being reimbursed the dispensed drug. Detail description on Drug Reimbursement report generation and sending phases is found in Appendix B 10.

Phase P1 and P2 are performed daily for each treatment to a patient, and P3 and P4 are performed monthly to prepare and send the File F report to the Healthcare Authority for the drug reimbursement. This case study emphasizes on the drug prescription phase, and describes in detail the business objectives, business processes, assets, actors and risks of this phase.

For readability we introduce here dramatis personae of Drug Reimbursement scenario for a hospital in Italy which consists of different medical and surgical operational units.

- Ministry of Health is the responsible authority for providing healthcare service.

- HealthCare Authority is the responsible authority engaged by Ministry to guide hospital follow healthcare rules in providing medical service. It is also accredited to observe the Drug Reimbursement process of the hospital.
- Hospital is the authorized organization by the Ministry to provide medical service.
- Orthopedic Unit is an important operational unit of the hospital.
- Accounting Officer works for the Accounting office which is a sub-section of hospital engaged in generating Drug Reimbursement record.
- Medical Direction Unit is a sub-section of hospital engaged in generating Drug Reimbursement record.
- Hospital has a Pharmacy to store and maintain the drug stock.
- IT Office maintains the IT System of Drug Reimbursement process of the hospital.
- Bob is an outpatient of Orthopedic Unit.
- Alice as a doctor of Orthopedic unit appointed by hospital to prescribe drug to patient.
- Carry as a nurse of Orthopedic unit appointed by hospital for dispensing drug to patient.

Hospital requires personal and medical record of Bob (outpatient of Orthopedic Unit) to register him as a outpatient of Orthopedic unit and also to provide him (Bob) medical service. So, it (hospital) asks the permission from Bob for using his personal and medical record as by law Bob is the owner of his sensitive information. Bob has given permission to hospital for accessing his personal and medical information with condition on protecting privacy. Bob's personal and medical information is stored in hospital's IT system which is maintained by the IT Officer.

The Drug Reimbursement phase of the hospital starts with the Prescription phase when Bob (patient) has come to hospital for getting medical service. Alice (doctor of Orthopedic unit) identifies Bob as an outpatient of Orthopedic unit

through his personal or clinical record which is stored in hospital IT system. He (Alice) also retrieves all the previous medical records of Bob using the IT System of hospital and chooses the right drugs to prescribe him (Bob) by considering his past medical records. Finally Alice prints the prescription sheet, sign it and give it to the Bob. The prescription phase ends by archiving the prescription of the Bob to use in the dispensation and report generation phase.

Then Bob goes to Carry who is a nurse of Orthopedic Unit for getting drug. The dispensation phase is conducted by Carry where she checks the prescription given by Alice (doctor) and dispenses drug from the available drug stock. She also stores the dispensed drug record.

Accounting Officer engages in generating report and sending it to the Healthcare Authority which is the last phase of Drug Reimbursement process. The Drug Reimbursement reports are generated from the Drug Prescription and Drug Dispensation information. Hospital Pharmacy checks the prescription and dispensation records and helps the Accounting office in identifying gaps between the records (if exists). The reports are sent to the Healthcare Authority by Medical Direction Unit.

Chapter 2

Actor Modeling

2.1 Constructs

The first step towards modeling an organization is to identify the stakeholders and the relationship between them. Organizational structure is used for this purpose. It helps to understand the architecture of an organization as by revealing the hierarchical concept of subordination of stakeholders in organization. Organizational structure/Organigram allows categorization of entities into groups or individuals and identification of allocated responsibilities over the entities considering the concept of branch, department, workgroup and individual. Tropos allows modeling the organizational structure through Actor Modeling which consists of identifying entities and analyzing hierarchical concept of subordination of entities within the organization.

2.1.1 Actor

In tropos stakeholders/entities related to an organization can be defined as Actor.

Definition 1. *Actor is an autonomous entity that has strategic goals and performs actions to achieve them.*

An actor generally can be a human agent or the position that human agent holds. It also can be a software agent since software agent has an intention which is originated from some human agents (i.e., users, stakeholders). Considering this Tropos allows two categories of actors: Agent and Role.

Definition 2. *An agent is an active entity with concrete manifestations and is used to model humans as well as software agents and organizations.*

Definition 3. *A role is the abstract characterization of the behavior of an active entity within some context.*

Figure 2.1 shows the graphical representation of agent and role in Tropos.

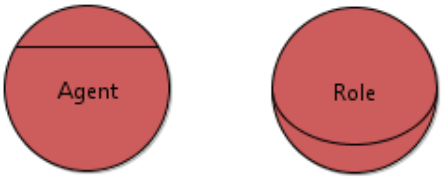

Figure 2.1: Graphical Representation of agent and role.

Example 2.1.1. This example considers the drug prescription phase of Drug Reimbursement process of hospital defined in scenario 1.4. We find the following entities related to drug prescription phase:

- Hospital
- Operational Unit
- Orthopedic Unit
- HealthCare Authority
- Doctor
- Patient
- Alice
- Bob

The entities defined above are considered as *Actors* as they have strategic desires and responsibilities to fulfill. Patient and doctor are the behavior or the position which are played by human being Alice and Bob. We can consider Alice and Bob as agent. Here the scenario does not consider any particular hospital. So hospital, operational unit, Orthopedic unit are modeled as *role* as they are abstract entities. We can divide the entities of hospital in drug prescription phase in following roles and agents defined in table 2.1:

Role	Agent
Hospital	
Operational Unit	
Orthopedic Unit	
Doctor	Alice
Patient	Bob
HealthCare Authority	

Table 2.1: Actor Identification from Drug Prescription phase of hospital 1.4

Remember 2.1.1. *In case of modeling an abstract concept (role) of organization, all the sub-components of it are also modeled as roles. Again, for modeling an organization as an active entity (agent), all the sub-components should be modeled as agents.*

2.1.2 Hierarchical Relation

Tropos captures the hierarchical structure and relationship between actors in the organization using "play", "is-a" and "supervise" relationships.

Play relation

In tropos, the relationship between an agent and a role is defined by "play" relation where agent is performing the role.

Example 2.1.2. In drug prescription scenario 1.4, Bob is a patient in the hospital and Alice is a doctor. We can model the situation that Bob is a patient in Tropos using "play" relation where Bob as an Agent playing the role of patient and the same way relationship between Agent Alice and role Doctor can be modeled with "play" relation. The graphical representation of "play" relation is found in figure 2.2.

Warning 2.1.1. *"play" relation always holds between an agent and a role. In scenario 1.4, Bob is an agent and patient is a role. So the relationship between agent Bob and role patient can perfectly described by "play" relation. On the other hand, the relationship between Operational Unit and Orthopedic Unit cannot be*

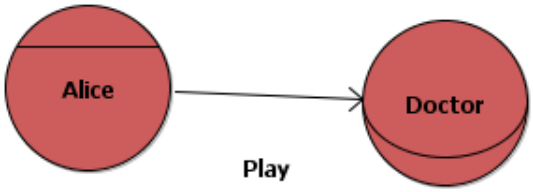

Figure 2.2: Play relation between agent and role.

modeled with "play" relation. This is because; both Operational Unit and Orthopedic Unit are roles as the scenario defines the hospital as abstract entity instead of mentioning any particular hospital scenario.

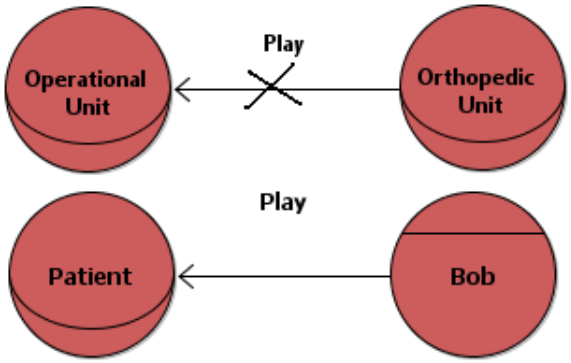

Figure 2.3: Incorrect example of Play relation.

"is-part-of" relation

"is-part-of" relation acts between two roles and is used to decompose complex roles into subcomponents such as the internal structure of an organization or the logical sub-components of a software agent.

Example 2.1.3. The relation between hospital and Operational Units can be modeled with "is-part-of" relation as Operational Unit is the sub-part of Hospital. The graphical representation of "is-part-of" relation is found in figure 2.4.

"is-a" relation

Tropos defines "is-a" relation to model the relationship between two actors indicating that an actor refers to more specialized activities of another actor. The

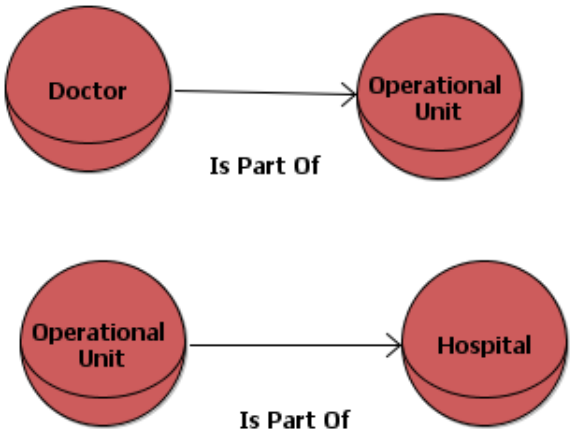

Figure 2.4: is-part-of relation between roles.

specialized actor inherits all properties of the generalized actor. This indicates that "is-a" relationship can hold between two roles or two agents and not between a role and an agent. This relation is employed to understand role specialization hierarchies.

Example 2.1.4. In scenario 1.4, Orthopedics unit is a specialized operational unit in Hospital. This indicates that Orthopedic unit includes all the facilities and responsibilities of a general operational unit in a hospital. Again, it can have some more functionalities and can provide medical facilities particularly to Orthopedic patients. The graphical representation of "is-a" relation is found in figure 2.5.

Warning 2.1.2. *"is-a" relationship only holds between two roles or between two agents. In scenario 1.4, the relationship between agent Bob and role patient cannot be modeled with "is-a" relation. This is because, Bob is an agent and Patient is a role.*

Tips 2.1.1. *A common mistake happens in identifying "is-a" and "is-part-of" relationship between the actors. In scenario, the relationship between hospital and operational units can be defined with "is-part-of" relationship. Operational Units are sub-components or the internal structure of a hospital, so here "is-part-of" relationship is suitable to define the relationship between a hospital and its operational units. Again, if we try to define the relationship between operational unit and Orthopedics unit with "is-part-of" relation considering that Orthopedic unit is a sub-component of operational unit then it will be a wrong interpretation of the*

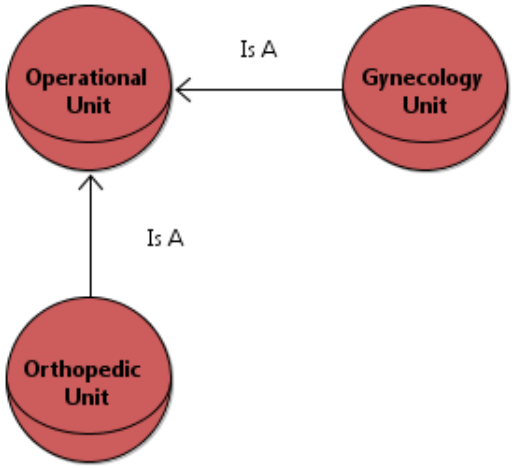

Figure 2.5: is-a relation between roles.

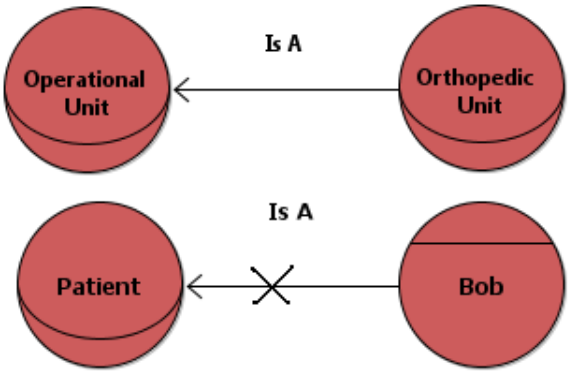

Figure 2.6: Incorrect example of is-a relation.

relationship between them. Actually Orthopedic Unit itself is an operational unit. It is considered as the specialization and not a sub-part of Operational Unit. The relationship between Orthopedic unit and operational unit should be defined with "is-a" relationship.

"supervise" relation

The relation of supervision between two roles can be defined by "supervise" relation in Tropos.

Example 2.1.5. In scenario 1.4, hospital needs to follow the regulation and guide-

lines for healthcare services provided by the HealthCare Authority. HealthCare Authority has the power and responsibility to evaluate and review hospital's services. The relationship between hospital and HealthCare Authority can be modeled with "supervise" relation. The graphical representation of "supervise" relation is found in figure 2.8.

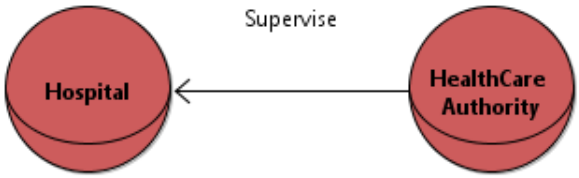

Figure 2.7: supervise relation between roles.

Warning 2.1.3. *A common mistake may happen to identify "supervise" and "is-part-of" relationship. It should be remembered that "supervise" relation is used between two roles where one role has the power and responsibility to evaluate and review the second role. On the other hand, "is-part-of" relation best suits to define relationship between two roles where second one is considered as the sub-component of the first role. In scenario 1.4, HealthCare Authority has the power and respon-*

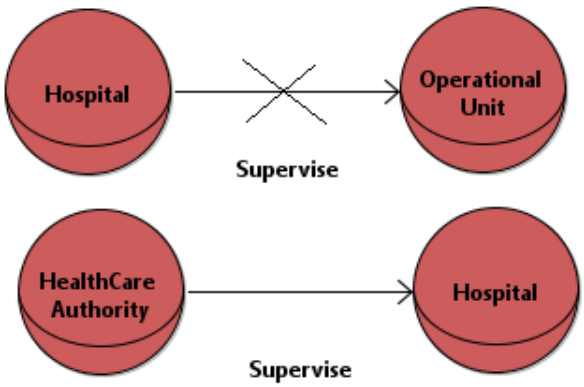

Figure 2.8: Incorrect example of supervise relationship.

sibility to evaluate and review hospital's services. The relationship between HealthCare Authority and hospital can be defined with "supervise" relation. Instead, "supervise" relationship is not suitable to model the relationship between hospital

and operational units. "is-part-of" is appropriate here as operational units are sub-components of hospital as operational units are sub-components of hospital.

2.2 Methodological Steps

The process for Actor Modeling is shown in figure 2.9.

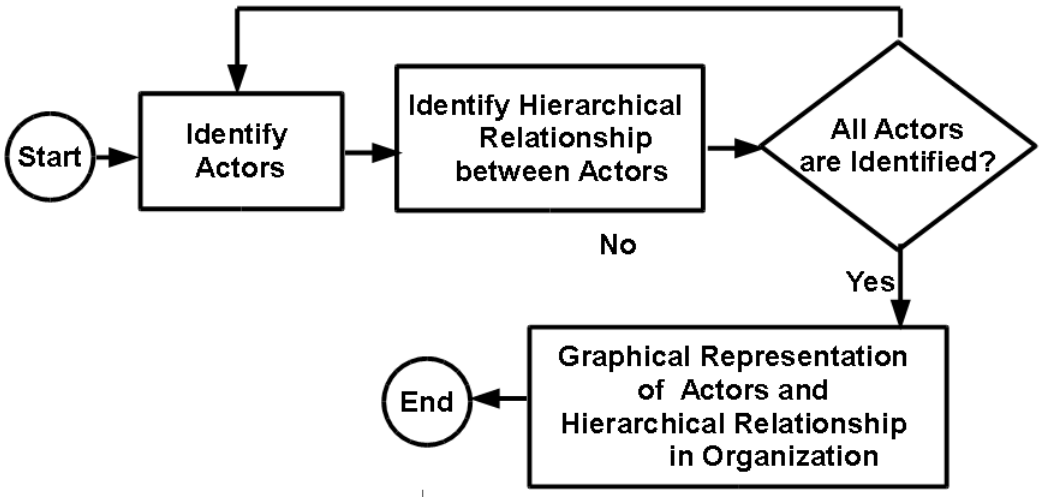

Figure 2.9: Process Diagram of Actor Modeling.

Step 1 - Actor Identification

All the actors in the organization need to be identified. Here actor indicates both the agent and the role. The input of this phase is the organizational structure or organigram.

Example 2.2.1. This example shows the steps of identifying the actors from the organizational structure. For this example we have chosen the hospital as an organization and the input of this example is the organigram of the hospital shown in Figure 2.10. This organigram refers to the hierarchy of management within a hospital. This is the strategic organizational structure which helps to understand the hospital's chain of command. This organigram does not consider the functional structure of the hospital. So instead of describing the functional position (doctors, nurses, etc.) the high level chain of commands are found in the organigram. In the organigram of figure 2.10, the nodes indicate the position and

responsible entity holding that position while link from one node to other indicate the hierarchy of positions in hospital management. To figure out the entities of

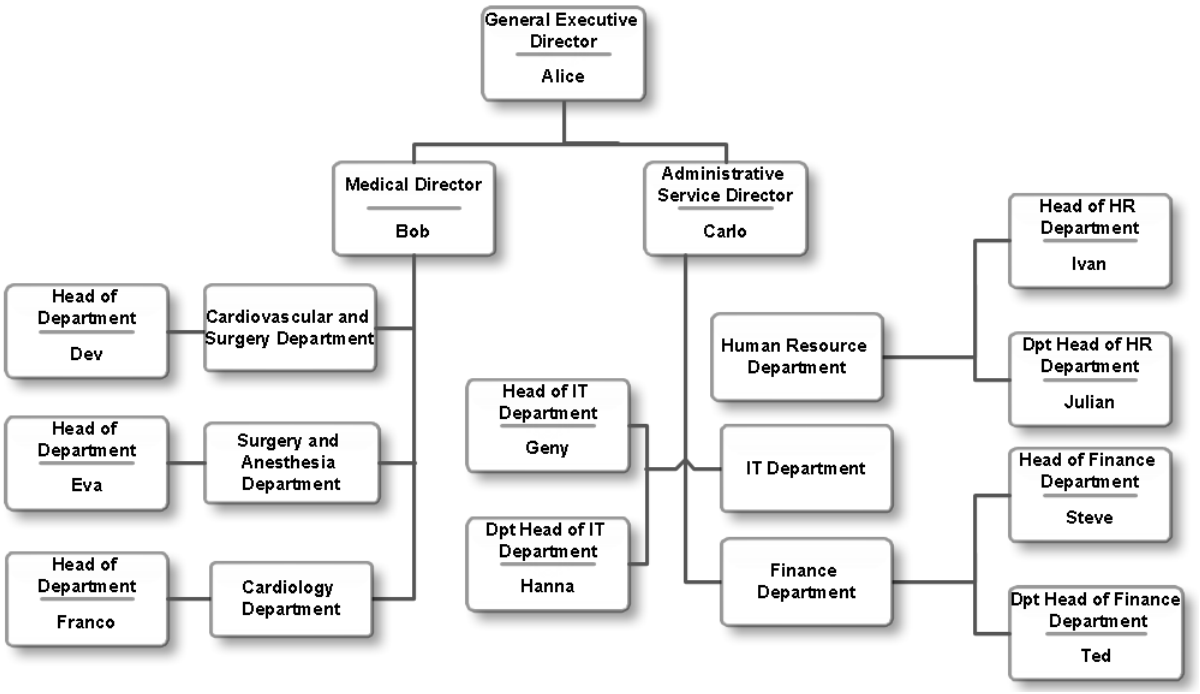

Figure 2.10: Organizational Structure of a Hospital

hospital management we need to consider all the nodes in the organigram. All the entities in the organigram whether they are active or abstract are considered as actors. From the organigram of figure 2.10, we have found **General Executive Director** is the top position or command of management in the Hostpital. In the second level of management we found two personnel **Medical Director** and **Administrative Service Director**. This indicates that the Hospital is divided into two sections according to the functionality it performs:

- Medical Section
- Administrative Service Section

Considering the chain of command in Hospital from organigram in figure 2.10, the identified roles and agents are: Among these actors, according to Tropos the abstract entities are defined as Role. The organigram in figure 2.10 deals with the generalized organizational structure of a hospital. As specific hospital is not

Role	Agent
Hospital	
Medical Section	
Administrative Service Section	
Cardiovascular and Surgery Department	
Surgery and Anesthesia Department	
Cardiology Department	
Human Resources Department	
IT Department	
Finance Department	
General Executive Director	Alice
Medical Director	Bob
Administrative Service Director	Carlo
Head of Cardiovascular and Surgery Department	Dev
Head of Surgery and Anesthesia Department	Eva
Head of Cardiology Department	Franco
Head of IT Department	Geny
Dpt of IT Department	Hanna
Director of Human Resources Department	Ivan
Dpt of Human Resources Department	Julian
Head of Finance Departmet	Steve
Dpt of Finance Department	Ted

Table 2.2: Actor Identification from Organigram mentioned in figure 2.10

mentioned here, so hospital and the departments of the hospital are considered as roles.

Remember 2.2.1. *It is to remember that, the human agents, software agents and specific organizations should be modeled as Agents. The position or the abstract role is considered as Role. Organigram in figure 2.10 defines the generalized organizational structure of a hospital so in Tropos the hospital and all it's departments should be modeled as roles. On the other hand, if the organigram in figure 2.10 represents the organizational structure of any specific hospital named "Hospital H" then it should be modeled as an agent in Tropos as it is an instance of the abstract entity hospital. Similarly all the departments of the "Hospital H" should also considered as agents.*

Warning 2.2.1. *Careful identification of agents and roles is required as wrong*

identification of roles and agents will lead to misinterpretation of the hierarchical relationship between actors.

Step 2:

The hierarchical relationships between the actors need to be identified. We can analyze the organigram to identify the responsible authority in the organization and also can figure out the heirarchical relationship between them.

Example 2.2.2. This examples describes the process of identifying the hierarchical relations from the organigram in figure 2.10. *General Executive Director* is found at the top in management chain in the hospital. *General Executive Director* is an abstract entity which is performing by *Alice*. The relationship between *Hospital* and *General Executive Director* can be defined by "is-part-of" relationship. We found "play" relationship between role *General Executive Director* and agent *Alice*.

The organigram of figure 2.10 shows complex organizational structures of the hospital. The hospital is divided into sub-components in order to ensure efficiency of service. Here grouping is done according to similarity of functionality. The organigram shows two sub-components in the hospital which are *Medical Section* and *Administrative Service Section* according to the functional similarity in the hospital. As the organigram deals with the general organizational structure of a hospital so here the sub-components of the hospital are also considered as roles. *Medical Section* and *Administrative Service Section* indicate the internal structure of the *Hospital*. In Tropos we can define "is-part-of" relationship between two agents or two roles to model the internal structure of the organization. So the relationship of these two sub-sections *Medical Section* and *Administrative Service Section* with *Hospital* can be modeled with "is-part-of" relationship.

If we consider the internal structure of the *Medical Section*, we found it is divided into six sub-departments which are *Cardiovascular and Surgery Department*, *Surgery and Anesthesia Department*, *Cardiology Department*, *Orthopedic Department*, *Gychonology Department* and *Diagonistic Department* according to the similarity of funcionality. These six sub-departments of *Medical Section* are also considered as roles as they are sub-components of a role *Medical Department*. This sub-departments expresses the internal structure of the *Medical Department*

and the relationship between *Medical Department* and each of these six departments can be defined by "is-part-of" relationship.

The chain of command of *Medical Section* in organigram shows that *Medical Director* is the top at management of this section. *Bob* is the *Medical Director* in the organigram. The relationship between agent *Alice* and role *Medical Director* can be defined with "play" relationship in actor diagram.

We have found six responsible persons as the head of the six departments under *Medical Section*. We can consider these positions as roles. *Dev* is the *Head of Cardiovascular and Surgery Department*. *Eva* is the *Head of Surgery and Anesthesia Department*. *Franco* is the *Head of Cardiology Department*. So the relationship between *Dev* and *Head of Cardiovascular and Surgery Department* can be defined by "play" relationship. Again "play" relationship can be used between *Eva* and *Head of Surgery and Anesthesia Department*, *Franco* and *Head of Cardiology Department*. The organigram shows the internal structure of *Administrative Service Section* which is divided into three sub-departments *Finance Departmet*, *Human Resources Departmet* and *IT Departmet*. These three departments indicate the internal structure of *Administrative Service Section* and can be modeled with "is-part-of" relationship in Tropos. In organigram, *Administrative Service Director* is the at the top of the management of *Administrative Service Section*. This role of *Administrative Service Director* is playing by *Carlo*. The relationship between *Administrative Service Director* and *Carlo* can be defined with "play" relationship. In the same way, "play" relationship holds between *Geny* and *Head of IT Department*, *Hanna* and *Dpt of IT Department*, *Ivan* and *Director of Human Resources Department*, *Julian* and *Dpt of Human Resources Department*, *Steve* and *Head of Finance Department* and *Ted* and *Dpt of Finance Department*. As the *Administrative Service Director*, *Carlo* has the power to monitor and supervise the work of *Head of IT Department*, *Director of Human Resources Department* and *Head of Finance Department*. So we can model the relationship with *Carlo* and *Geny* by "supervise" relationship. Again "supervise" relationship holds between *Calro* and *Ivan*, *Carlo* and *Steve*. Again, inside the sub-departments of *Administrative Service Section*, "supervise" relation holds between *Geny* as the Head of IT Department with *Hanna* as the Dpt of IT Department, *Ivan* as the Director of Human Resources Department and *Julian* as the Dpt of Human Resources Department, *Steve* as the Head of Finance Department and *Ted* as the Dpt

of Finance Department.

Step 3:

The Actor Diagram is produced representing the roles and agents participating to the system with hierarchical relationships between them.

Example 2.2.3. The actor diagram of the organigram is found in figure 2.11.

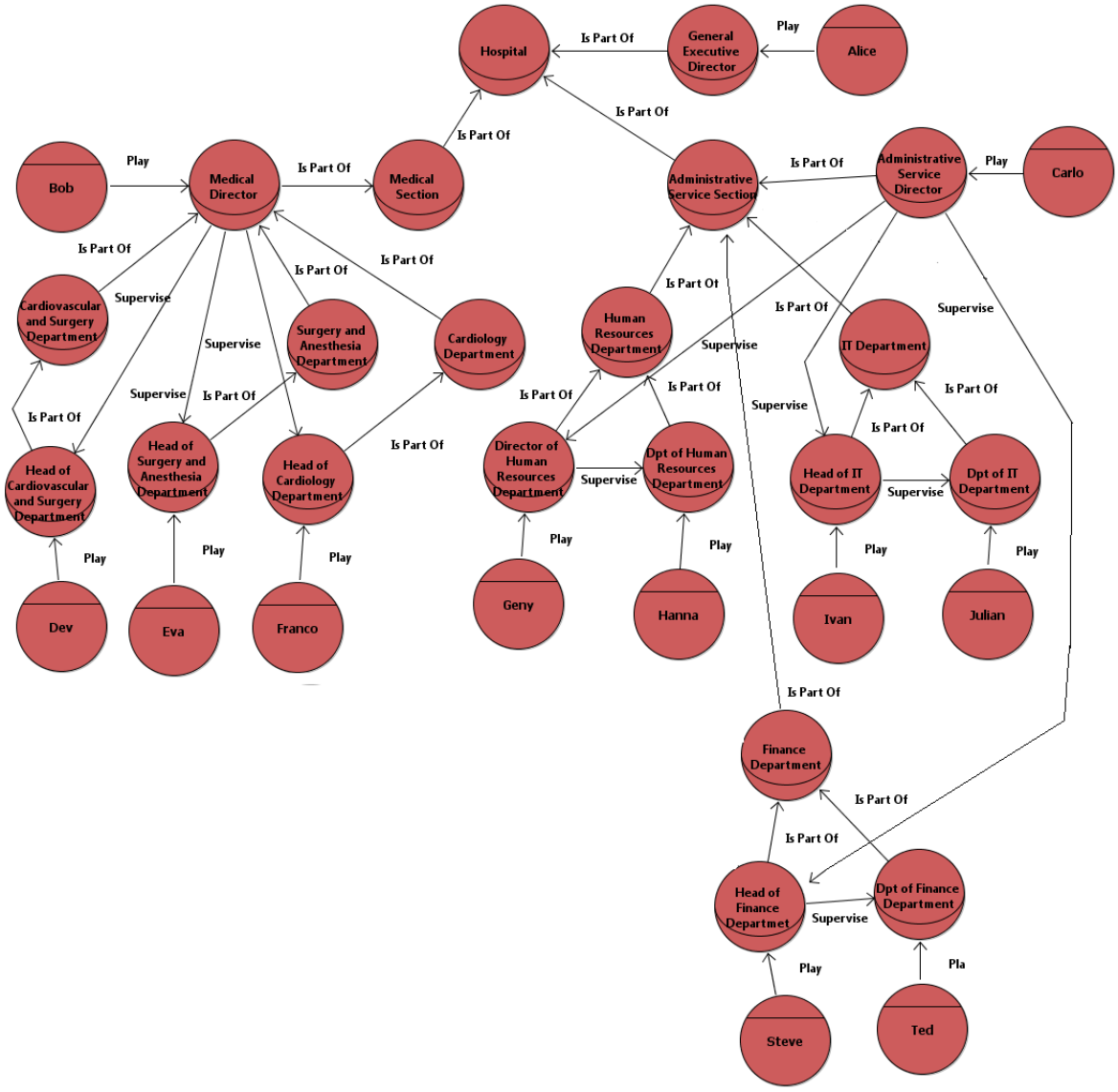

Figure 2.11: Actor Diagram of Drug Prescription Phase

Chapter 3

Goal Modeling/Functional Modeling

3.1 Constructs

In the organization, stakeholders have specific interests or responsibilities to perform and sometimes they need to execute other low level duties to fulfill their main desires/responsibilities.

Example 3.1.1. In Drug Reimbursement scenario 1.4, the responsibility of doctor in the hospital is to **Prescribe drug to patient**. To fulfill this responsibility, doctor needs to **identify patient**, **analyze patient's medical record** and finally **prescribe drug to patient** which can be considered as low level functionalities to achieve his main responsibility.

Identification of the strategic interests of the stakeholders (actors) is important for modeling of an organization. Functional modeling helps to understand the interests/motivations and responsibilities of entities in an organization. It identifies the motivations of the entities and decomposes them into low level functionalities which are needed to achieve to fulfill their interests/responsibilities. Tropos uses the notion of functional modeling and introduces the concept of Goal Modeling to capture the motivation, strategic interest and responsibility of the entities (actors) in the organization and also allows modeling the decompositions and delegation of the responsibility.

3.1.1 Goal

In Tropos the motivation or the intentional desire of an actor in the organization is defined as goal.

Definition 4. *Goal as a state of affair which an actor intends to be achieved.*

Example 3.1.2. In Drug Reimbursement scenario 1.4, the main responsibility of the doctor in the hospital is to prescribe drug to patients. So **Prescribe drug to patient** can be defined as the goal of the doctor.

The graphical representation of the goal in Tropos is found in figure 3.1. Tropos

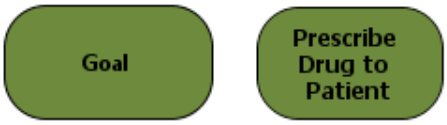

Figure 3.1: Graphical Representation of Goal.

divides goals into two categories (e.g., Hard and Soft goal) according to the satisfaction criteria of the goal.

- Hard Goal - This can be considered as the responsibility/interest of the actor for which the satisfaction criteria is well defined.

  Example 3.1.3. In Drug Reimbursement scenario 1.4, **Prescribe drug to patient** is a hard goal as it is functional and the satisfaction criteria for this goal is well defined. This goal is fully achieved if doctor prescribes drug to the patient.

- Soft Goal - In the organization, entities may have "special" type of non-functional motivations having no clear-cut definition and/or criteria for deciding whether they are satisfied or not. These non-functional requirements can be modeled with the concept of **soft goal**. These goals (soft goal) can be treated as criteria or preference that an actor desires to be achieved.

  Example 3.1.4. In Drug Reimbursement scenario 1.4, doctor in the hospital desires to get patient's satisfaction with his treatment, behavior, etc. But it is hard to define the exact criteria to gain patient's satisfaction. So, **Achieve patients' satisfaction** can be modeled as a soft-goal.

The graphical representation of Soft-Goal is found in figure 3.2.

Figure 3.2: Graphical Representation of Soft Goal.

Remember 3.1.1. *Hard Goal is precise and its end state or outcome is clearly specified. Examples of goals are: Patient Be Prescribed, Product Be Designed, Payment be done etc. Soft-goals should be used to model quality attributes or non-functional requirements or when stakeholders' goals are not precise or their criteria of success are not sharply defined in advance. Examples of soft-goals are:* **Get patients' satisfaction**, **Design Process Be Efficient**, **Low Product Cost** *etc. For example* **Efficient Technique** *suggests that it is likely to be a soft-goal, not a goal as it is not precise, or it's criteria of success are not sharply defined in advance. The criteria to achieve the soft-goal* **Design Process Be Efficient** *is subject to interpretation. Conversely,* **Product Be Delivered** *is highly likely to be a hard goal because the Customer is either get the delivery of the product or not. If the Customer is concerned about the timely delivery of the product, then this new requirement would be modeled as a soft-goal,* **Timely Delivery of Product**. *We need to remember that the distinction between a (hard) goal and a soft-goal is not in the degree of importance. To model something as a soft-goal is not to say that it is less important, or that it is optional.*

3.1.2 AND Decomposition, OR Decomposition

Tropos allows decomposition and refinement of top level responsibilities of entities into low level functionalities. Through goal refinement Trpos captures the scenario where actors need to perform low-level functionalities to furnish their responsibilities, using goal decomposition. To model a finer goal structure, a root (high-level) goal can be decomposed into sub-goals using AND/OR decomposition.

- AND Decomposition - It refines a goal (G) into sub-goals that must be satisfied in order to achieve the top-level-goal (G).

Example 3.1.5. Figure 3.3 shows the example of AND decomposition from Drug Reimbursement scenario 1.4. Here the top level goal of doctor **Prescribe Drug to patient** can be decomposed into following sub-goals **Identify Patient**, **Prescribe Drug**, **Finalize Prescription phase** using AND decomposition. To achieve the top goal **Prescribe Drug to patient** doctor needs to satisfy all the three decomposed sub-goals.

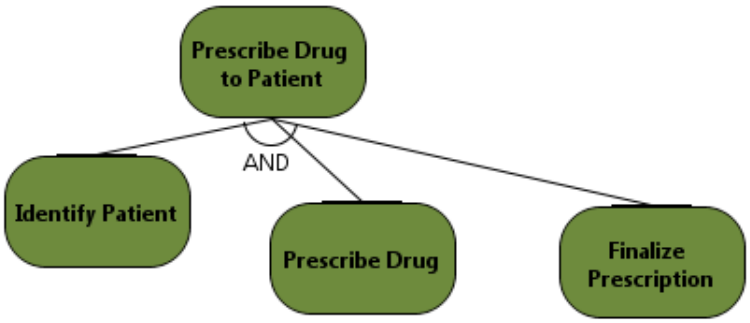

Figure 3.3: AND decomposition of top level goal.

- OR Decomposition - This type of decomposition is used to design alternatives to achieve top-level-goal. In OR decomposition it is sufficient to achieve only one of the sub-goals.

  Example 3.1.6. Figure 3.4 shows the example of OR decomposition from Drug Reimbursement scenario 1.4. Here, the goal of doctor **Identify Patient** can be satisfied either by **Identification by Patient's Tax Code** or **Identification by Patient's Clinical Record**.

3.1.3 Objectives, Entitlements and Capabilities

In organization, there exists complex relationships between goals and the actors which are captured by the notion of ownership and permission. Here the goal is desired by some actor, can be realized by some (possibly different) actor, or is controlled by some (possibly different) actor. Similar complex relations are also observed in between actors and their plans or actors and resources where *plan* and *resource* can be defined as Task and Resource 5.1 in Tropos.

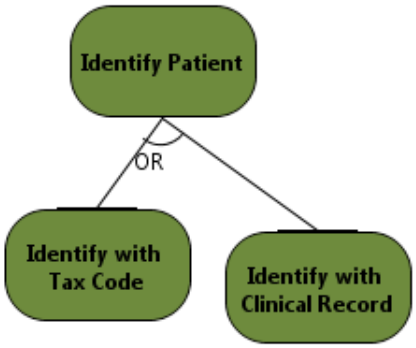

Figure 3.4: OR decomposition of top level goal.

Example 3.1.7. In Drug Reimbursement scenario 1.4, a patient's desire is to get medical service (be prescribed). But he is not capable to fulfill his goal by himself. The patient depends on hospital for his treatment and the hospital appoints doctor as he is capable to fulfill a patient's goal by prescribing him drug.

Again, the doctor needs to access patient's personal information to identify him as a outpatient of operational unit and his medical record to provide him drug. But doctors don't have access to the patient's persional and medical information as by law patient is the owner of his personal and medical information. So doctors here act as data requesters. The hospital stores the patients' information as patients allow it to use their medical and personal information and makes it available to doctors of the operational unit. Accordingly, the hospital acts as a data provider here.

Tropos captures this complex situation where the actors who are capable of fulfilling goals or execute tasks or deliver resources are different from the ones who are entitled to do that and both are different from the actors who want the perform that. It defines three properties of a goal/task/resource as Objectives, Entitlements and Capabilities to analyze the relationship between actors and goal/task/resource.

- Objective denotes the motivation of actors where actor wants a goal to be achieved or a plan to be executed or a resource to be delivered.
- Entitlement denotes the ownership of a goal/plan/resource for an actor where the actor has full authority concerning the achievement of his goal, execution of his plan, or use of his resource.

- Capability denotes the scenario where actor has the ability and knowledge necessary to achieve a goal or execute a plan or furnish a resource.

In Tropos the Objectives, entitlements and capability property is denoted as (R)equest, (O)wn and (P)rovide. Request denotes the objectives of actors, Own denotes the entitlements of actors and Provide denotes the capabilities of actors. In graphical diagrams, Request, Own and Provide can be represented as edges between an actor and a goal or a resource or a task labeled with R, O and P, respectively. Figure 3.5 shows the graphical representation of Request, Own and Provide.

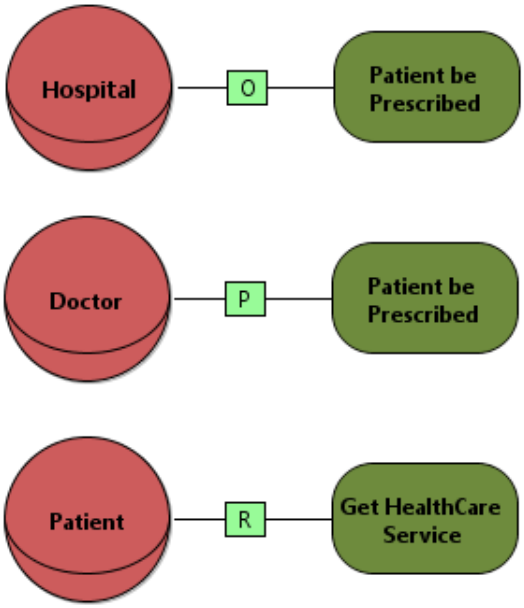

Figure 3.5: Graphical representation of Request, Own and Provide.

3.1.4 Delegation

The concept of ownership and permission brings the idea of *dependency* into light. An actor might not have all capabilities to fulfill his goals and tasks. He depends on other actors to perform his job. Thus, dependency between two actors indicates that one actor depends, for some reason, on the other in order to attain some goals, execute some tasks, or to produce resources.

Tropos introduces the notion of **Delegation** to deal with this issue to model the social dependency for defining the obligations of actors to other actors. **Delegation** is used to model the transfer of responsibilities from an actor to another.

Definition 5. *Delegation (among two actors and a service(goal/task/resource)), marks a formal passage of objective or authorization.*

Here, Delegation modeling consists of identifying actors which delegate other actors the permission and task of execution on goals, plans, and resources. The former actor is called the *delegater*, while the latter is called the *delegatee*. The object around which the dependency centers is called *delegatum*. In a delegation, the *delegater* depends on the *delegatee* to bring about a certain state of affairs or to perform a activity or to produce a resource. The *delegatum* is expressed as an assertion statement. The *delegatee* is free to, and is expected to, make whatever decisions are necessary to achieve the goal or execute the task or to produce the resource *delegatum*. The *delegater* does not care how the *delegatee* goes about achieving the goal. Tropos allows two types of delegation:

- **Delegation of Execution** - Used to model formal passage of responsibility. Tropos uses the concept of *Delegation Execution* to model the transfer of objectives from an actor to another. Explicitly it indicates that one actor (the depender) appoints another actor (the dependee) to achieve a goal or execute a task or furnish a resource (the dependum). *Delegation Execution* does not indicate the transfer of rights/ownership of a goal/task/resource. As consequence of delegation execution, the *delegatee* wants the achievement of the goal or the execution of task or the delivery of the resource.

  Example 3.1.8. In Drug Reimbursement scenario 1.4, the objective or motivation of the hospital is to **prescribe drug to patient**. But the hospital does not have capabilities to fulfill this goal and it depends on the doctor to perform this goal. The doctor is capable to **prescribe drug to patient**. So, the hospital appoints doctor to fulfill its goal **prescribe drug to patient**. This issue can be modeled with the concept of **Delegation Execution (De)** shown in figure 3.6.

- **Delegation of Permission** - Used to model formal passage of authority. The notion of *Delegation of permission (Dp)* is used to model the actual

Figure 3.6: Delegation Execution in Drug Prescription phase.

transfer of rights of goal/task/resource (delegatum) from one actor (delegater) to other (delegatee). Details on *Delegation of permission (Dp)* is found in chapter 6.

Remember 3.1.2. *In general, by depending on another actor for a delegatum, an actor is able to achieve goals that it would otherwise be unable to achieve on its own, or not as easily, or not as well. At the same time, the delegater becomes vulnerable. If the delegatee fails to deliver the delegatum, the delegater would be adversely affected in its ability to achieve its goals.*

3.2 Methodological Steps

Goal modeling is the analysis of high level goals from actors' perspective. It also allows the discovery of alternative sets of lower level goals to achieve top level goals. Particularly Goal modeling divides into two phases: Goal Elicitation and Goal Refinements.

3.2.1 Step 1: Goal Elicitation

Goal Elicitation is identifying the goals of all actors in the organization. In this step we need to consider the responsibility, motivation and intension of all the actors in the organization and defined them as goals. In re-engineering process, the business objectives of the organization need to be analysed to find out the responsibilities and motivations of the actors.

3.2.2 Step 2: Identify Strategic Dependency

The strategic dependencies among the actors in the organization need to be identified. Strategic dependency depicts the dependencies between Actors in the orga-

nization. In the re-engineering process the strategic dependencies can be identified through the business objectives, business process, critical success factors.

3.2.3 Step 3: Goal Refinement

Goal Refinement represents the process of goal decomposition into the lower level goals. Goal Refinement can be done by any of the following ways:

- Critical success factor - High level goal can be decomposed into low level goals considering the Critical Success Factor of the organization. Critical success factors are the functionalities required to ensure the achievement of the organizational objectives.
- Intermediate Goal - Goal Refinement can also be done by identifying the intermediate goal to achieve the desire of the actor.
- Business Process - In the re-engineering process, Goal Refinement can be done through the identification of sub-goals from existing business process of the organization.

The ECO(Entitlements, Capabilities, Objectives) property of the goal plays important role in goal refinement process. In Goal Refinement process, for each goal of an actor the ECO(Entitlements, Capabilities, Objectives) property should be defined. If the actor is not capable to achieve the goal by himself then actor can either decompose the goal to subgoals or can assign other actor for satisfying the goal for him. If the actor is the owner of the goal then he is considered the owner for all the decomposed sub-goals. Otherwise, for all the decomposed sub-goals the owner needs to be defined.

The goal decomposition can be done with AND/OR decompositions, where AND decomposition defines that sub-goals must be acheived to achieve the parent goal, while OR decomposition defines choice amongh the sub-goals to achieve the parent goal. The process for goal refinement is found in figure 3.7.

Remember 3.2.1. *The goal decomposition can be done till all the leafe goals can be performed by the owner of the goal or delegated to other actors.*

Example 3.2.1. This example defines the goal modeling (elicitation and decomposition) of Drug Reimbursement process of hospital defined in scenario 1.4. The

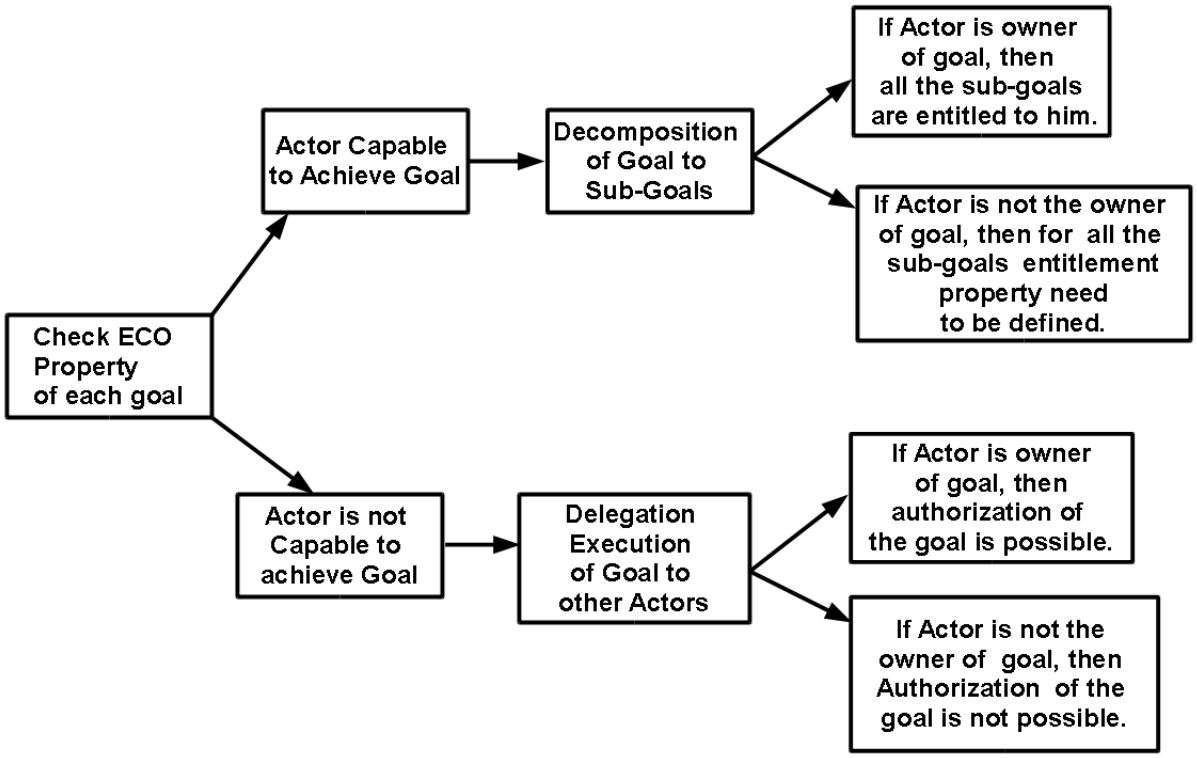

Figure 3.7: Goal Refinement process of Goal Modeling

first step is identification of goals which indicates the identification of the motivations and responsibilities of the actors. To simplify the example, we here describe the identification of goals in a single actors rationale (i.e., the hospital can be seen as a "big" actor). As this is a re-engineering process, we can focus on the business objectives of the Drug Reimbursement process to find out the top-level responsibility of the hospital. The main business objective of the hospital is to **Provide Medical Service**. From the business process of Drug reimbursment it is found that hospital has to carry out the following responsibilities to achieve the main business objective.

- Prescribe drug to patient.
- Dispense drug to patient.
- Generate drug reimbursement report.
- Send drug reimbursement report to HealthCare Authority.

- Being reimbursed by HealthCare Authority.

These sub-responsibilites can be modeled as the decomposed sub-goals of main goal **G01-Provide Medical Service** of the hospital. Now, we can proceed towards further refinement of these sub-goals. But it is observed that hospital is not capable to perform all these jobs by itself. So hospital delegates the sub-goals **G02-Prescribe drug to patient**, **G03-Dispense drug to patient** and **G04-Generate drug reimbursement report** and **G05-Send drug reimbursement report** to other actors. Figure 3.8 shows the identification and refinement of goals of the hospital. The goal **G02-Prescribe drug to patient** is delegated to doctors

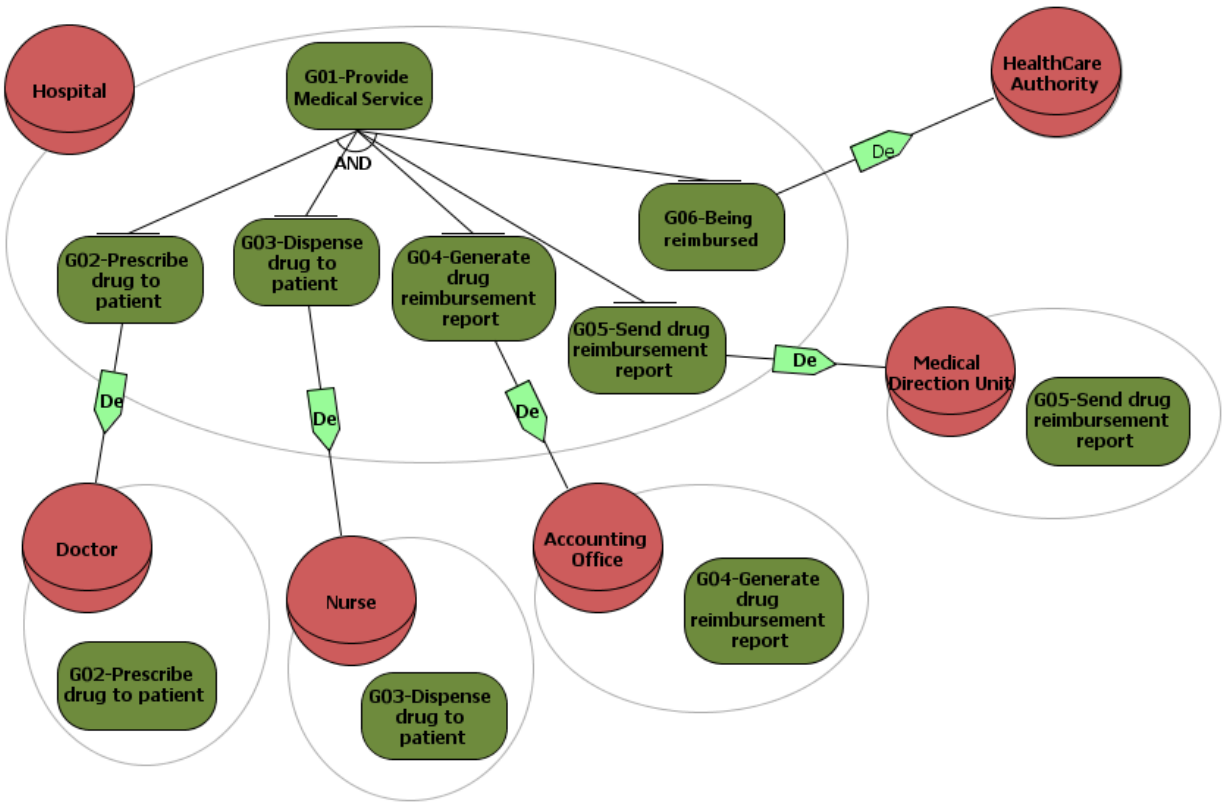

Figure 3.8: Goal Identificatin and Refinement in Drug Reimbursement phase

and it then becomes the responsibility of doctor. Nurse/doctor in the operational unit are appointed to perform the goal **G03-Dispense drug to patient**. The goal **G04-Generate drug reimbursement report** is delegated to the Accounting Office and it is added as a responsibility of the accounting office. The Medical

Direction Unit is appointed to execute the goal **G05-Send drug reimbursement report**.

We need to refine the goals of every actors till all the leafe goals can be performed by the owner of the goal or delegated to other actors. But, here for simplicity, we are describing only the further goal refinement of the goal **G02-Prescribe drug to patient** which is delegated to the doctor by the hospital. Through the *delegation execution*, the goal **prescribe drug to patient** is delegated to doctor and he gets the permission to adopt any suitable means to perform this job. But it is noticed that, here only the responsibility of the execution of the goal is transferred, not the authorization. So, doctor is not the owner of this goal. The doctor only can delegate this job **prescribe drug to patient** or sub-parts of it to others but cannnot transfer the authorization as he is not the owner of the job. For the refinement of the goal **G02-Prescribe drug to patient**, we need to observe the business processes of drug prescription phase in Appendix A 9 to identify other responsibilities of the doctor to fulfill this goal. The business process of Drug Prescription in scenario is found in figure 3.9. Inorder to prescribe drug to patient, the doctor first needs to identify the patient using the patients' personal information stored in the operational unit. He analyses patient's previous medical record to understand his health condition and choses appropriate drug for the patient. Then he delivers the prescription to patient and archieve the prescription sheet. So the main goal **G02-Prescribe drug to patient** of doctor in hospital is divided into following three sub-goals :

- Identify Patient (G07) - From the case study of drug prescription phase (in Appendix A 9), we have found two alternatives to achieve this goal.
  - Identify Patient by Tax Code (G10)
  - Identify Patient by Clinical Record (G11)
- Prescribe Drug (G08)
- Finalize Prescription phase (G09) - From the case study of drug prescription phase (in Appendix A 9), we have found two sub-goals to finalize the prescription phase.
  - Deliver Prescription to patient (G12)

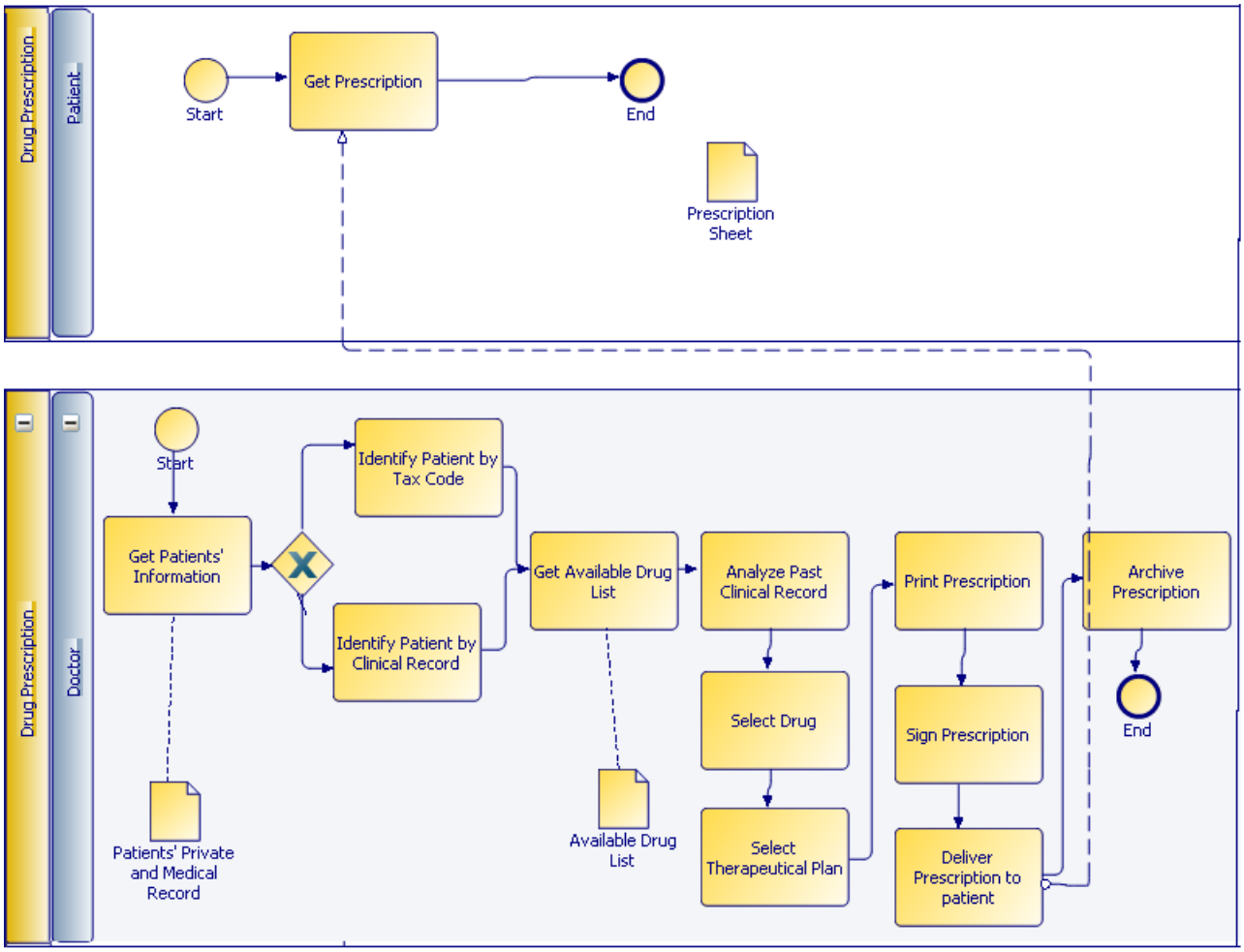

Figure 3.9: Business Process of Drug Prescription in Hospital

– Archive Prescription (G13)

The refinement of the goal **G02-Prescribe drug to patient** of the doctor ends here as G10, G11, G12, G13 are the smallest sub-goals to achieve the main goal and can be achieved by the doctor himself with the help of some resources (e.g., patients' info). G10, G11, G12, G13 are considered as leaf-goals in the goal model. Figure 3.10 shows the refinement of the goals of doctor in Drug Prescription phase.

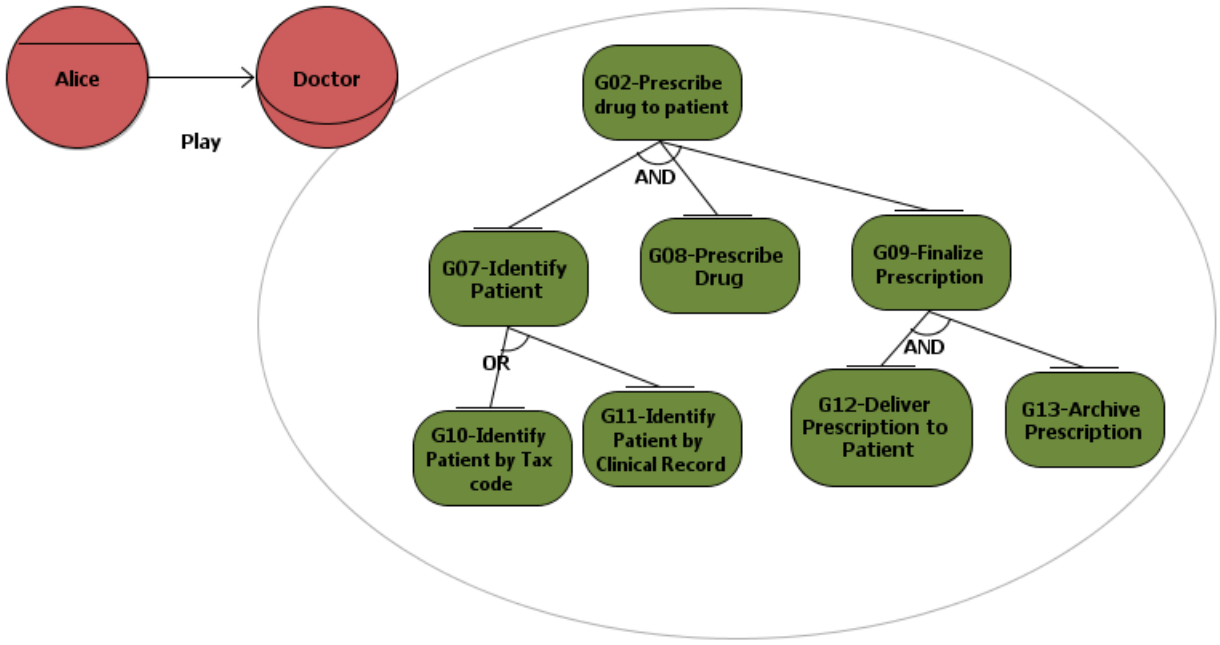

Figure 3.10: Goal Refinement in Drug Prescription phase

Chapter 4

Trust Modeling

4.1 Running Example

The example is based on the compliance of Italian public administrations such as universities, local governments and health care authorities to Italian security and privacy legislation. In summary, the law requires administrations to set up sophisticated security and privacy policies that are actually quite close to the complexity of the ISO-17799 standard for security management. Dealing with privacy introduces additional complications such as data ownership, trust and consent. Details on the case study for an university can be found in [**?**]. For readability we introduce here dramatis personae:

- Bill is a student of Faculty of Science in University A.
- Alen is an administrative officer of University A.
- Sam is (the manager of) the student IT system of University A.

Bill is the owner of his personal information such as academic record. As a student he needs to submit his personal information to the University A. Sam as the manager of the student IT system, seeks the permission from Bill for data processing concerning his personal data. Alen is interested in gathering data on student performance, for which he depends on Sam.

4.2 Constructs

Tropos introduces the notion of *delegation* to model the formal passage of responsibility/authority to achieve a goal or to execute a task or to deliver a resource from one actor to another. Particularly, Sub-section 3.1.4 introduces the concept of *delegation execution* which is used to model the transfer of responsibilities from an actor to another. Chapter 6 represents *delegation permission* to model formal passage of authority from one actor to other.

In Tropos *delegation* indicates that one actor (*delegator*) transfer the responsibility/authority to another actor (*delegatee*) to achieve a goal or execute a task or furnish a resource (*delegatum*). Depending on actors for a service makes the *delegator* vulnerable. To simplify terminology, the notion of *service* is used in this framework to refer to a goal, task, or resource. Actually, the *delegatee* may not achieve the assigned responsibilities even if he has committed it. Similarly, the *delegator* has no warranty that the *delegatee* does not misuse the granted permission.

Example 4.2.1. In the University scenario of section 4.1, Alen (administrative officer) delegates the execution of his goal **Access students' personal and academic information** to Sam (manager of IT system). This delegation of responsibility is modeled with *delegation execution*. But, here, Alen cannot guarantee that Sam is able to complete his assigned responsibility. Again, Bill (student) gives permission to Sam (manager of IT system) to use his personal and academic information. This delegation of authority is modeled with *delegation permission* and it does not display Bill's believe that Sam is able to protect privacy of his information and does not misuse the granted permission.

Delegation does not necessarily depict the transfer of *trust* from *delegator* to *delegatee* on *delegatum*. This complex scenario introduces the necessity to separate the concepts of **trust** and **delegation** in modeling the organization. Tropos uses the separate concept of *delegation* and *trust* to model the formal and informal delegation of authority and responsibility. This separation allows the modeling of systems where some actors must delegate permission or assign responsibilities to untrusted actors.

4.2.1 Trust

In Tropos, *Trust* marks a social relationship that indicates the belief of one actor that another actor will not misuse the service he has been granted.

Definition 6. *Trust is a relation between two actors representing the expectation of one actor about the capabilities and behavior of the other.*

Trust relationship is hold among two actors and a service (goal/task/resource), so that an actor A trust another actor B on a certain goal G/ task T/ resource R and believes that he (actor B) does not misuse the service (goal G, plan T, or resource R). Here, actor A is called the *truster*, while actor B is called the *trustee*. The object (goal G/ task T/ resource R) around which the dependency centers is called *trustum*.

Warning 4.2.1. *In general, by trusting another actor for a trustum, an actor is sure that the trustum is properly used. At the same time, the truster becomes vulnerable. If the trustee misuses the trustum, the truster cannot guarantee to achieve some goal, execute some plan, or deliver a resource securely.*

Tropos captures the social dependency between actors in the organization using Trust Modeling. Tropos distinguishes two types of trust relations:

- **Trust of execution** - *Trust of execution* models the *trustor's* expectations concerning the ability and dependability of the *trustee* in achieving a goal or executing a task or delivering a resource. By trusting in execution, the *trustor* is sure that the *trustee* accomplishes the *trustum*.

  Trust of execution is represented as edge labeled with **Te**. The graphical representation of *Trust of execution* between two actors on a service (goal/task/resource) is found in figure 4.1.

Figure 4.1: Graphical Representation of Trust of Execution.

- **Trust of permission** - Trust of permission models the *trustor's* expectations that the *trustee* does not misuse a service (goal/task/resource). By trusting in permission, the *trustor* is sure that the *trustee* does not abuse the (possible) received permission for accomplishing a purpose different from the one for which the permission has been granted.

  Trust of permission is represented as edge labeled with Tp. The graphical representation of *Trust of permission* between two actors on a service (goal/task/resource) is found in figure 4.2.

Figure 4.2: Graphical Representation of Trust of Permission.

Example 4.2.2. In the University scenario of section 6.1, Bill (student) is the owner of his personal and academic data by law. Yet, University requires Bill's personal and academic information and the data is stored on servers that are managed by Sam (manager of IT system). Sam should seek the consent of (or, permission from) Bill for data processing concerning his personal and academic data. Bill delegates permission of using his personal and academic information to Sam, on condition that his privacy is protected (i.e., his identity is not revealed). Bill believes that the Sam will not misuse the permission of using his (Bill's) sensitive information and will keep privacy. Here, Bill is the the *trustor*, Sam is the *trustee* and Bill's personal and academic information is the *trustum*. The trust relationship between Bill and Sam can be modeled with *Trust Permission* in figure 4.3.

Again, Alen (administrative officer) needs to access Bill's (student) personal and academic information for administrative purpose. But he (Alen) depends on IT system manager Sam to achieve his goal. Alen trusts on the ability of Sam and believes that he (Sam) will accomplish the goal *Access to student's personal and academic record*. Here, Alen is the the *trustor*, Sam is the *trustee* and the goal *Access to student's personal and academic record* is the *trustum*. The trust

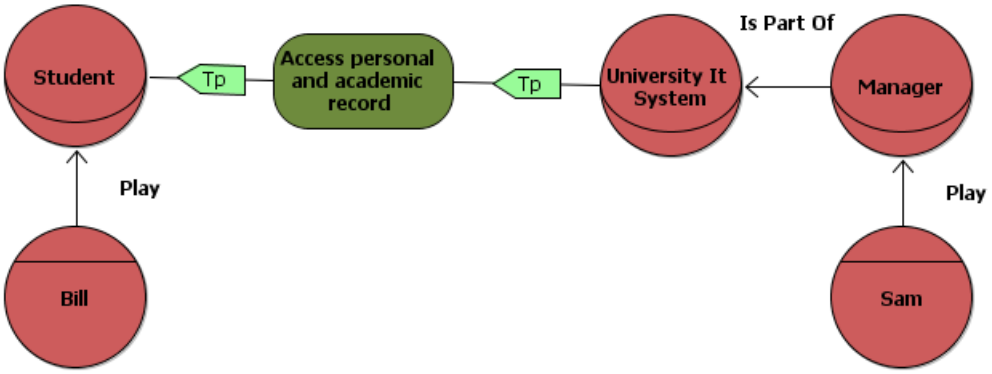

Figure 4.3: Example of Trust of Permission from University scenario 6.1.

relationship between Alen and Sam can be modeled with *Trust Execution* in figure 4.4.

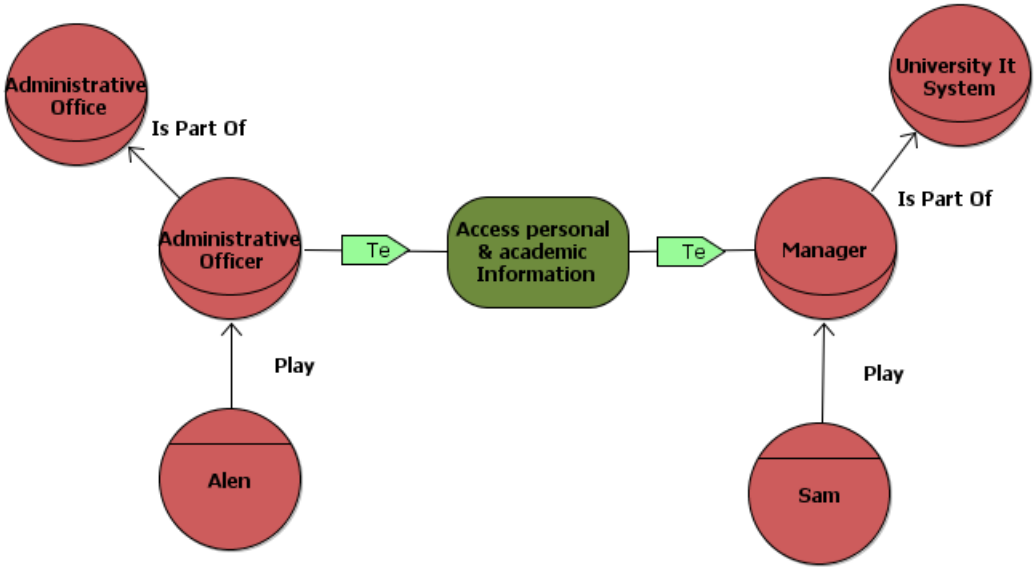

Figure 4.4: Example of Trust of Execution from University scenario 6.1.

4.2.2 Trust vs Delegation

This section mentions the distinction between *trust* and *delegation*. Tropos separates the concept of *Trust* and *Delegation*. Delegation is an action due to a decision,

whereas trust is a mental state driving such decision. So, in other words, *Trust* can be considered as the mental counterpart of *delegation*. In general, delegation marks a formal passage in the domain. This would be matched by the issuance of a delegation certificate such as digital credential or a letter if we are delegating permission or by a call to an external procedure if we are delegating execution.

Example 4.2.3. In the University scenario of section 6.1, Bill is the owner of his personal data by law. Yet, the data is stored on servers that are managed by Sam. Sam should seek the consent of (or, permission from) Bill for data processing concerning his personal data. The agreement papers with signature of Bill that assures the permission of using sensitive (personal and academic) data for academic purpose is an example of delegation of permission.

In contrast, trust marks simply a social relationship that is not formalized by a "contract" (such as digital credential or a letter). There might be cases (e.g. because it is impractical or too costly), where we might be happy with a "social" protection, and cases in which formal delegation is essential. Such decisions are taken by the designer and the formal model just offers support to spot inconsistencies.

4.3 Methodological Steps

Trust modeling consists of modeling the trust relation between actors in the organization. This section mentions the methodological steps of Trust Modeling.

Step 1:

Trust modeling starts with the identification of the actors who trust other actors for achieving a goal or executing a task or delivering a resource. Analysis on social relationship between actors can be helpful to identify the trust relationship between actors in the organization.

We need to identify actor (*trustor*) who delegates the execution of his goal or task or resource to other actor (*trustee*) with believe that he has the capability to perform service and will do his (*trustee*) best to fulfill the delegated service. This trust relation is modeled with *trust execution*.

We also need to identify the actor *trustor* who delegates the authority of his goal/resource/task to other actor *trustee* with believe that he will not misuse the permission and does not abuse the (possible) received permission for accomplishing a purpose different from the one for which the permission has been granted. This trust relation is modeled with *trust permission*.

Step 2:

After the identification of the actors and services among which the trust relationships exist in organization, we need to represent them with the graphical representation of *trust execution* and *trust permission*.

Example 4.3.1. This example shows the process of Trust Modeling of Drug Reimbursement scenario 1.4. The Ministry of Health is the responsible authority to provide healthcare service to patient. The Ministry delegates the authority of the goal **Provide Medical Service** to hospital. A relationship of trust can be noticed between Ministry of Health and hospital where the Ministry has faith that hospital will take essential decisions to fulfill the goal **Provide Medical Service**. It (Ministry) believes that the hospital will not misuse the authorization for any illicit means. This trust relation can be modeled with *trust permission*.

Through the *delegation permission* of the goal, now hospital becomes the owner of the goal **Provide Medical Service** and is authorized to make any decision to achieve this goal. The main goal of the hospital **Provide Medical Service**, can be decomposed into sub-goals **Prescribe Drug to Patient**, **Dispense Drug**, **Generate and Send Drug Reimbursement report** and **Being Reimbursed**. It (hospital) can delegate the execution of sub-goals to other actors as it (hospital) is not capable to fulfill all of them. For example, hospital is not capable to accomplish the goal **Prescribe Drug to Patient** which is a sub-goal of the main goal **Provide Medical Service**. Hospital delegates the execution of this goal **Prescribe Drug to Patient** to doctor. It (hospital) appoints doctor as it believes that the doctor is able to perform the goal **Prescribe Drug to Patient** appropriately. This trust relation between hospital and doctor can be modeled with *trust execution*. Similarly, hospital engages Accounting office for the finishing the goal *Generate Drug Reimbursement report* and Medical Direction unit for *Sending Drug Reimbursement report*.

Again, in Drug Reimbursement scenario, Patients are the owner of their personal and medical information by law. But hospital requires patients' personal and medical information for patient identification and treatment purpose. So the hospital seeks patients' consent for processing their personal and medical data. Bob as a patient of Orthopedic Unit gives permission to hospital for accessing his personal and medical information with the condition that privacy is protected. Bob (patient) believes that hospital doesn't misuse his sensitive information. Here, Bob is the *trustor* has faith on hospital *trustee* that it (hospital) does not abuse the (possible) received permission for accomplishing a purpose different from the one (administrative and treatment purpose) for which the permission has been granted. The trust relationship between Bob (patient) and hospital can be modeled by Trust of Permission relation. The graphical representation of Trust Model of Drug Reimbursement scenario is found in figure 4.5.

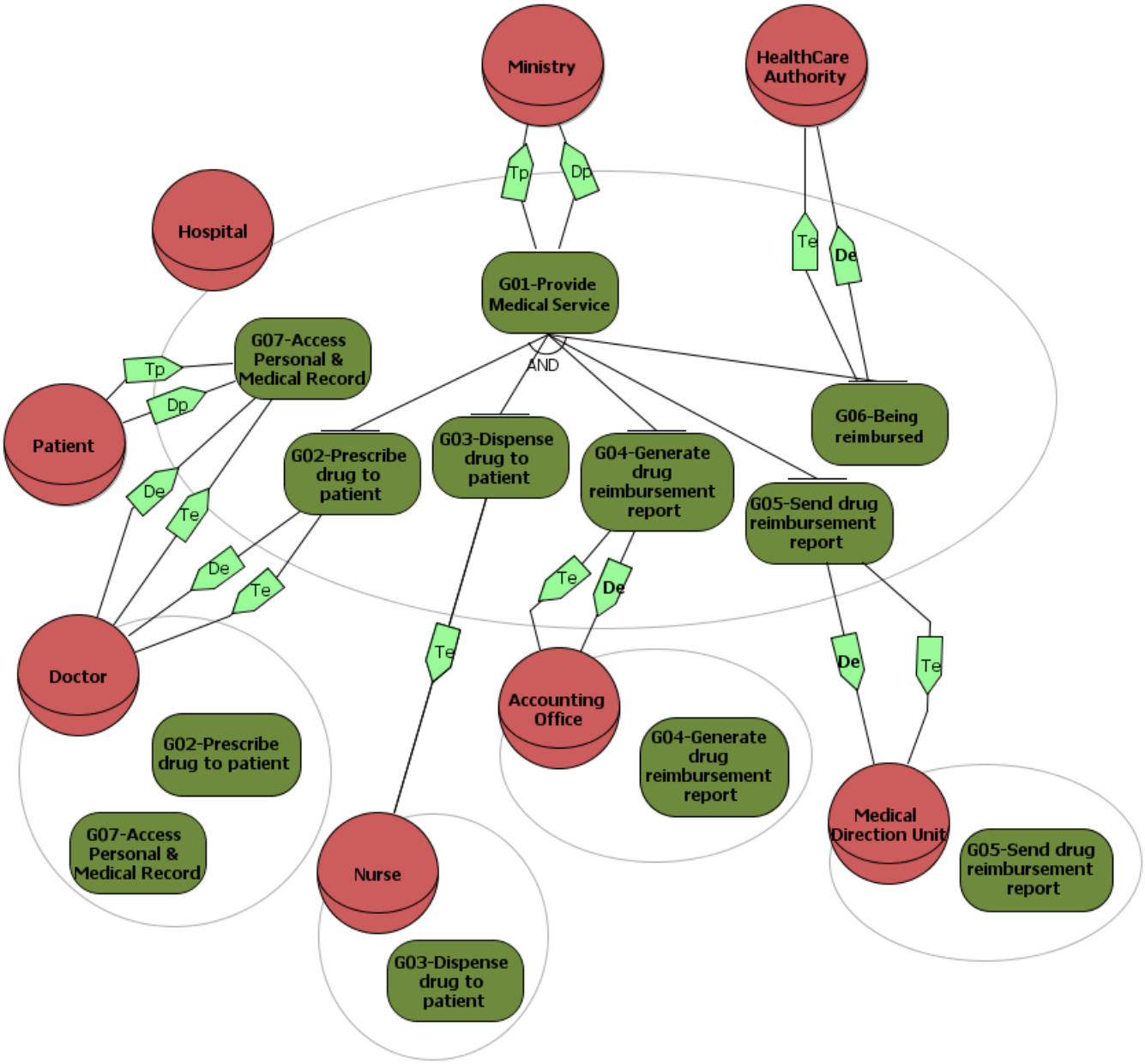

Figure 4.5: Example of Trust Modeling of Drug Reimbursement process.

Chapter 5

Process Mapping

5.1 Constructs

Section 3 describes the process of goal refinement into sub-goals until the leaf-goals can be achievable by delegating to other actors or by means of some activities. This section represents the modeling of activities/tasks actors need to execute to fulfill their desires in the organization.

Example 5.1.1. In Drug Reimbursement scenario 1.4, the doctor's responsibility is to prescribe drug to patient. He can fulfill his responsibility by means of identifying patient, analyzing medical record of patient and prescribing drug with appropriate therapeutically plan.

Tropos allows modeling the activities which are the means to achieve goals with Process mapping.

5.1.1 Task

Tropos defines activity which is required to achieve business objective as Task.

Definition 7. *Task captures a course of actions that results in a desired state. A task can be executed to satisfy some goals or to produce some resources.*

Example 5.1.2. In Drug Reimbursement scenario 1.4, to satisfy the goal **Prescribe Drug** the doctor needs to execute the activities **Analyse Medical Record** and **Select Drug and therapeutic plan**. These two activities can be defined as **Task** in Tropos.

5.1.2 Resource

Tropos modeled the physical or information artefact with the concept of resources.

Definition 8. *Resource represents a physical or information artefact.*

Example 5.1.3. Again in Drug Prescription scenario 1.4, to identify Bob as a patient of Orthopedic unit, Alice as a doctor needs to access the patients' personal information stored in Orthopedic unit. Here, patients' personal and clinical record is required to achieve the goal of identifying and prescribing patient. In Tropos definition, we can identify Patients' Personal and clinical record as Resource.

Remember 5.1.1. *A resource can be considered as an entity without any intention. The main difference with an agent is that a resource has not intentionality.*

5.1.3 Means-end Relation

Tropos defines the relation between the task and goal with Means-End relation. Here, the task is described as "Mean" to achieve the goal which is the "End".

Definition 9. *Means-End is used to identify task or resource that provides a means to achieve a goal. It is also used for indicating a task that produces a resource.*

Figure 5.1 shows the graphical representation of task and means-end relation between tasks and goal. The means-end relationship is represented with an arrow starting from task ends to the goal.

Example 5.1.4. In Drug Reimbursement scenario 1.4, the activities **Verify Prescription & Dispenastion record** and **Generate Drug Reimbursement report** can be considered as the *means* to achieve the goal **Generate Drug Reimbursement report**. Figre 5.2 shows the graphical representation of means end relation between task and goal.

In Tropos Means-End can be used to describe the resource required to achieve the goal or to execute task. In Drug Reimbursement scenario 1.4, **Patients' Personal and Medical information** is considered as resource which is the means to achieve goal **Identify Patient**. Figure 5.3 shows the graphical representation of resource and means-end relation between goal and resource.

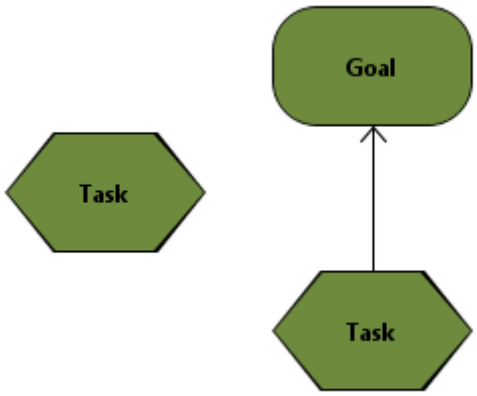

Figure 5.1: Graphical Representation of Tasks, Resource and Means-End relation.

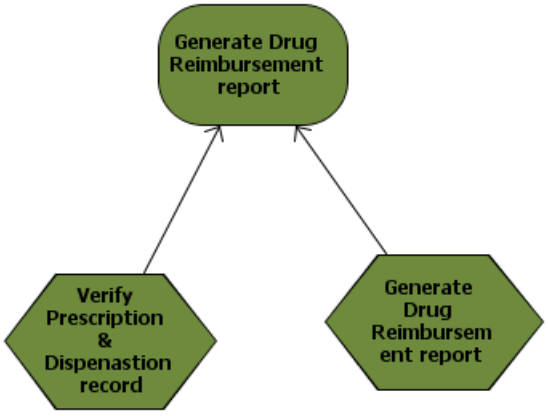

Figure 5.2: Example of Means-End relation.

5.2 Methodological Steps

This section aims to describe the methodological steps of Process Mapping.

Step 1: Identification of Tasks and Resources

The input of process mapping phase is the business processes and business objectives of the organization. which define the activities require to achieve business objectives/goal of the organization. Analyzing the business process we can identify process/activities of actors required for achieving business objectives. These activities are defined as **tasks** and can be modeled as **means** to achieve specific

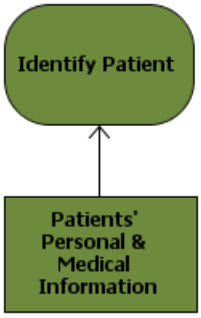

Figure 5.3: Graphical Representation of Means-End relation between goal and resource.

business objectives/goals. Analysis on the business process also reveals the physical or information entities which are required by actors to fulfill goals or to execute tasks. We also need to identify physical or information entities those are produced by the actors as a result of achieving goals or performing tasks. These physical or information artefacts can be modeled as **resources**.

Example 5.2.1. This example describes the process of identifying tasks of the actors from the business process of the organization. For simplicity, in this example only the Drug Prescription phase of Drug Reimbursement scenario 1.4 is considered. The main business objective of the doctor in drug prescription phase is to **Prescribe Drug to patient**. This objectives/goal can be decomposed into sub-goals and Goal Modeling 3 gives us a finer structure (in figure 5.4) of the goals of doctor in Drug Prescription phase. To find out the required activities we can analyze the business process of Drug Prescription phase (in figure 5.5) from Appendix A 9. From the business process of figure 5.5 of Drug Prescription phase, we have identified that following activities need to be performed by doctor to achieve his responsibility. To achieve the goal **Prescribe Drug** he needs to perform following activities which can be defined as tasks:

- ▷ Analyze Patient's Past Clinical Record
- ▷ Select Drug and therapeutical plan

Again to fultill the goal of **Deliver Prescription to patient** doctor needs to perform following tasks:

- ▷ Print Prescription

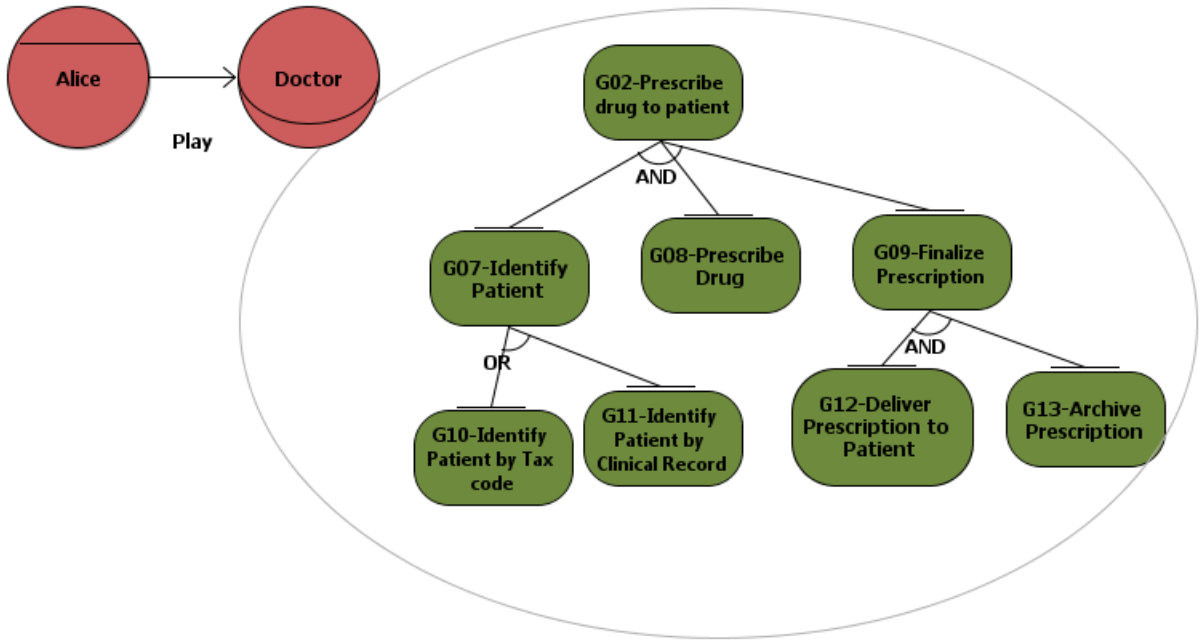

Figure 5.4: Doctor's Goal in Drug Prescription phase.

▷ Sign Prescription

From the business process of figure 5.5, the physical or information entities can also be identified which can be modeled as resources. Doctor in the hospital requires **Patients' Personal and Medical Information** to **Identify Patient (G07)** and also to execute the task **Analyse Patient's Past Clinical Record**. To perform the task **Selct Drug and therapeutical plan** the doctor need the available **Drug List of Operational Unit**. Again, the result of execution of the task **Print Prescription** is the **Prescription Sheet**. Moreover, **Prescription Sheet** is required to fulfill the goal **Deliver Prescription to Patient (G10)** and **Archive Prescription (G11)**. So, following **resources** are found from above discussion in Drug Prescription phase:

▷ Patients' Personal and Medical Information (R01)

▷ Drug Information of Operational Unit (R02)

▷ Prescription Sheet (R03)

Figure 5.6 shows mapping of activities in the business process with the goals of a doctor the prescription phase.

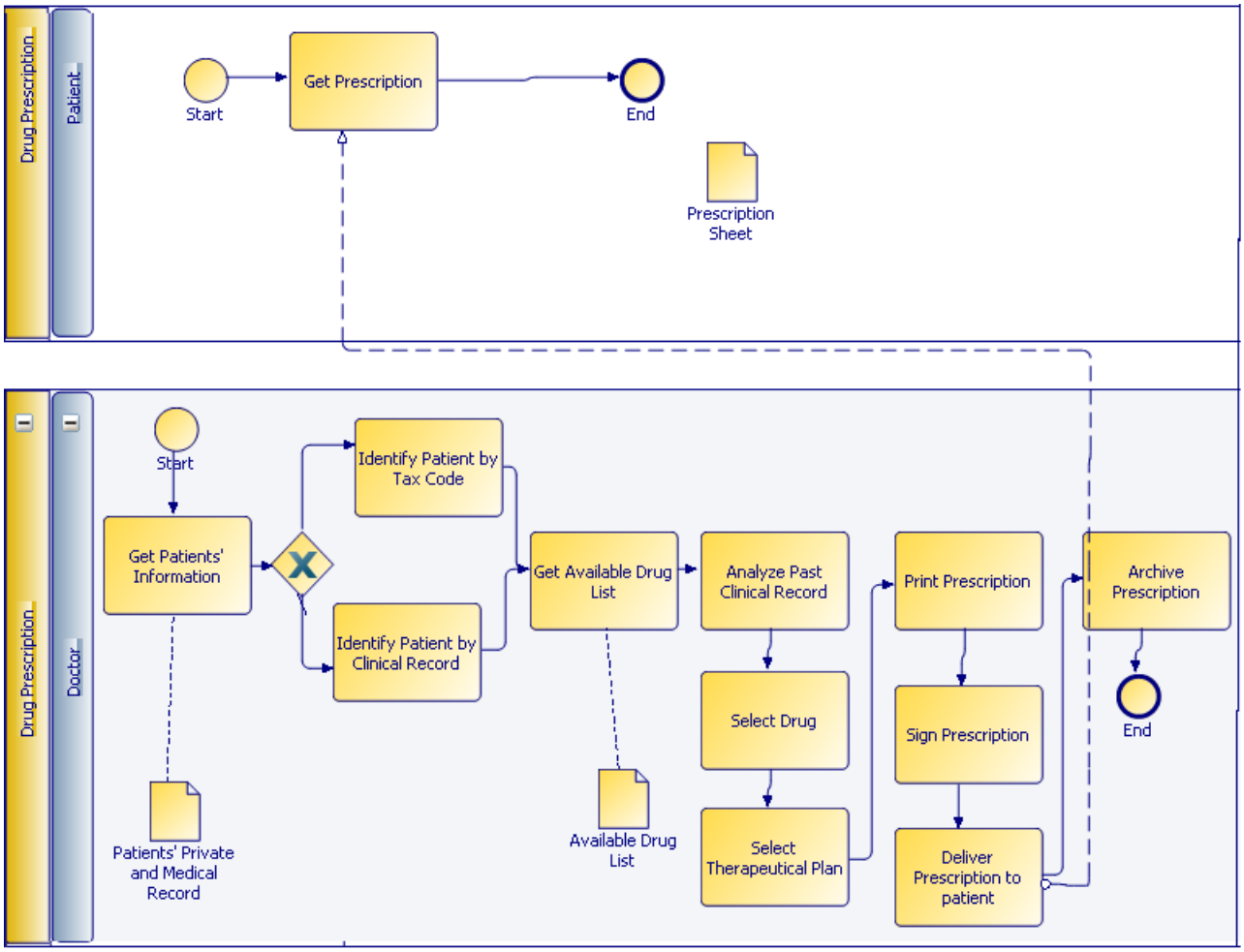

Figure 5.5: Business Process of Drug Prescription.

Step 3:

After identification of tasks and resources from the business process, we need to represent them in Tropos modeling environment using means-end relationship.

Example 5.2.2. Figure 5.6 shows the mapping of tasks and resources with the goal level. The graphical representation of the process mapping of the drug prescription phase is found in figure 5.7.

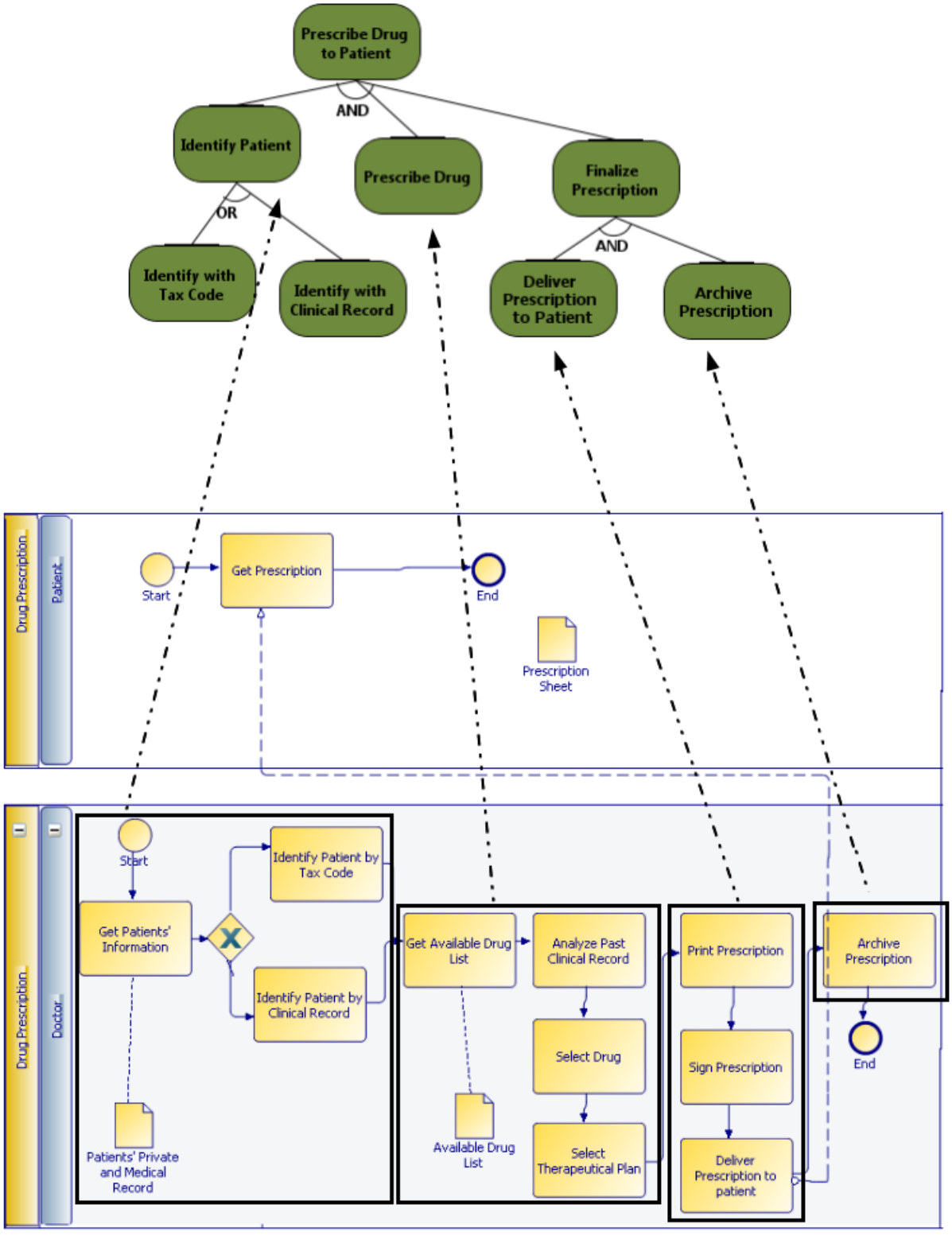

Figure 5.6: Process Mapping from business process model to goal level.

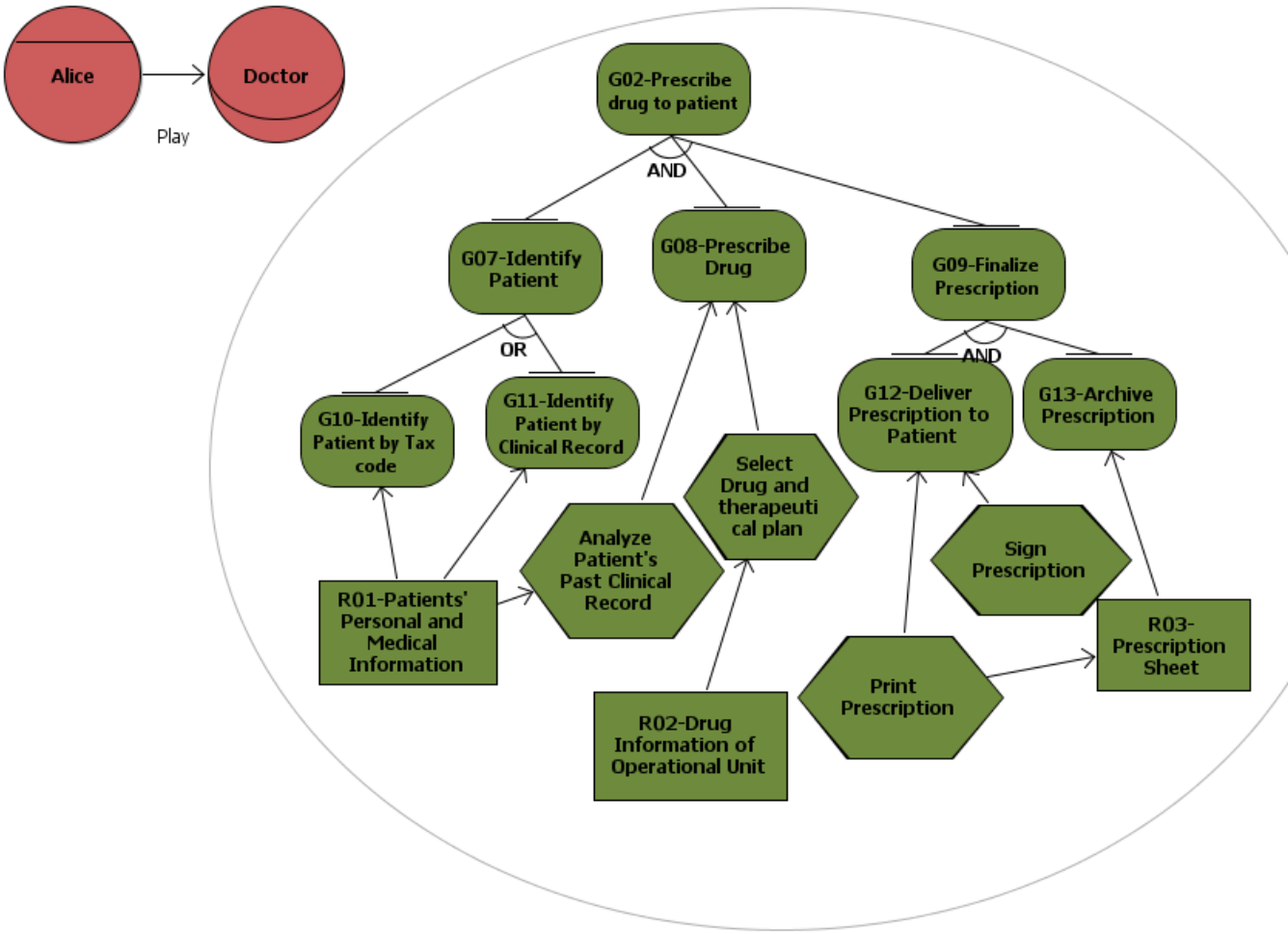

Figure 5.7: Example of Process Mapping.

Chapter 6

Permission Mapping

6.1 Running Example

The example is based on the compliance of Italian public administrations such as universities, local governments and health care authorities to Italian security and privacy legislation. In summary, the law requires administrations to set up sophisticated security and privacy policies that are actually quite close to the complexity of the ISO-17799 standard for security management. Dealing with privacy introduces additional complications such as data ownership, trust and consent. Details on the case study for an university can be found in [**?**]. For readability we introduce here dramatis personae:

- Bill is a student of Faculty of Science in University A.
- Alen is an administrative officer of University A.
- Sam is (the manager of) the student IT system of University A.

Bill is the owner of his personal information such as academic record. As a student he needs to submit his personal information to the University A. Sam as the manager of the student IT system, seeks the permission from Bill for data processing concerning his personal data. Alen is interested in gathering data on student performance, for which he depends on Sam.

6.2 Constructs

In the organization, complex relations may exist between actors and services. To simplify terminology, the notion of *service* is used in this framework to refer to a goal, task, or resource. Here, an actor might not able to fulfill his desire while other actor may have the capability to perform it. So, in organization one actor delegates to the other the permission to achieve some goal, execute some plan, or use a resource.

Tropos introduces the notion of *delegation* to deal with this issue. Chapter 3 describes the concept of *delegation* which is used among two actors and a service(goal/task/resource) to model a formal passage of permission. Particularly sub-section 3.1.4 introduces the notion of *delegation execution* which is used to model the transfer of objectives from an actor to another. But *delegation execution* does not indicate the transfer of rights/ownership of a goal/task/resource. This chapter represents the modeling of the actual transfer of rights of a service (goal/task/resource) from one actor to other. To model the transfer of rights of a service (goal/task/resource), we need to understand the notion of *Ownership*, *Provisioning* and *Requiring* which helps us to recognize the requester of a service, the legitimate owner of a service and provider of a service.

- **Ownership** - The concept of *Ownership* is used to describe the relationship between an actor and a service (goal/task/resource). It indicates that the actor is the legitimate owner of some goal, some plan, or some resource. The owner has full authority concerning to achieve his goal, execute his plan, or use his resource, and he can also delegate this authority to other actors.

- **Provisioning** - Provisioning indicates that the actor has the capability to achieve some goal, execute some plan, or deliver a resource.

- **Requiring** - Requiring indicates that the actor has the desire to achieve some goal, execute some plan, or deliver a resource.

Example 6.2.1. In the University scenario of section 6.1, Bill (student) is the owner of his personal and academic data by law. Yet, University requires Bill's personal and academic information and so the data is stored on servers that are managed by Sam (manager of IT system). Again, Alen (administrative officer) requests Sam to him Bill's personal and academic information for administrative

purpose. Here, Bill is the owner of the goal **Provide Personal and Academic Information**. Alen can be considered as requester of the goal **Provide Personal and Academic Information** as he depends on Sam to fulfill his goal. Sam can be considered as the provider of the goal **Provide Personal and Academic Information**.

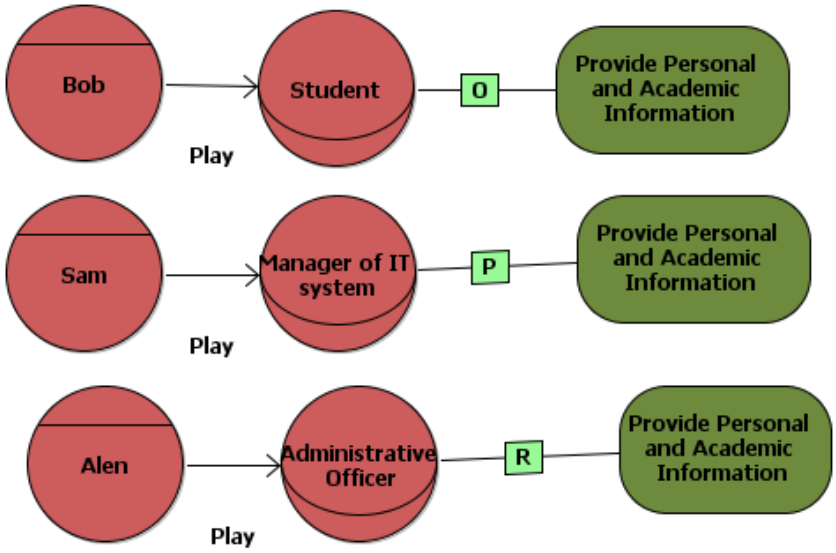

Figure 6.1: Graphical Representation of Delegation Permission of scenario.

Tropos uses the notion **Delegation Permission (Dp)** to model the formal passage of authorization from one actor to other.

Definition 10. *Delegation Permission indicates that one actor (the delegator) authorizes another actor (the delegatee) to achieve a goal or execute a task or deliver a resource (the delegatum).*

Example 6.2.2. In the University scenario of section 6.1, Bill is the owner of his personal data by law. Yet, the data is stored on servers that are managed by Sam. Sam should seek the consent of (or, permission from) Bill for data processing concerning his personal data. The agreement form with signature of Bill that assures the permission of using sensitive (personal and academic) data for academic purpose is an example of delegation of permission.

The graphical representation of *Delegation Permission* between two actors and a service (goal/task/resource) is found in figure 6.2.

Figure 6.2: Graphical Representation of Delegation Permission.

Example 6.2.3. In university scenario defined in this chapter, Alen (administrative officer) is interested in gathering data on student performance, for which he depends on Sam (manager of the student IT system). Bill (student) owns his personal data, such as his academic record. Bill delegates permission to provide information about his academic record to Sam, on condition that his privacy is protected (i.e., his identity is not revealed). Here, due to different types of delegation differences in the relationships between Alen - Sam and Bill Sam are noticed. Considering the relationship between Bill and Sam, it is found that Bill delegates permission to Sam to provide only the relevant information and nothing else. This situation can be modeled with *Delegation Permission*. On the other hand, Alen, who wants student data, delegates the execution of his goal to Sam which can be modeled as *Delegation Execution*. According to Alen, Sam should at least fulfill the goal he wants. He is not interested in whether Bill trusts Sam, he simply wants information. Bill, on the other hand, worries about authorization: anyone who uses his personal must be authorized to do so. Figure 6.3 shown the graphical representation of *delegation* relationships of this scenario.

As consequence of permission delegation, the *delegatee* is authorized to achieve the goal or perform a task or deliver the resource. The *delegatee* is free to, and is expected to, make whatever decisions are necessary to achieve the goal or execute the task or to produce the resource *delegatum*. He *delegatee* can also delegates the authorization (delegation permission) or responsibility (delegation execution) of the goal/task/resource to other actor if he is not capable to fulfill it.

Example 6.2.4. In Drug Reimbursement scenario 1.4, the Ministry of Health is the responsible authority to provide healthcare service to patient. The Ministry delegates the authority of this goal **Provide Medical Service** to hospital.

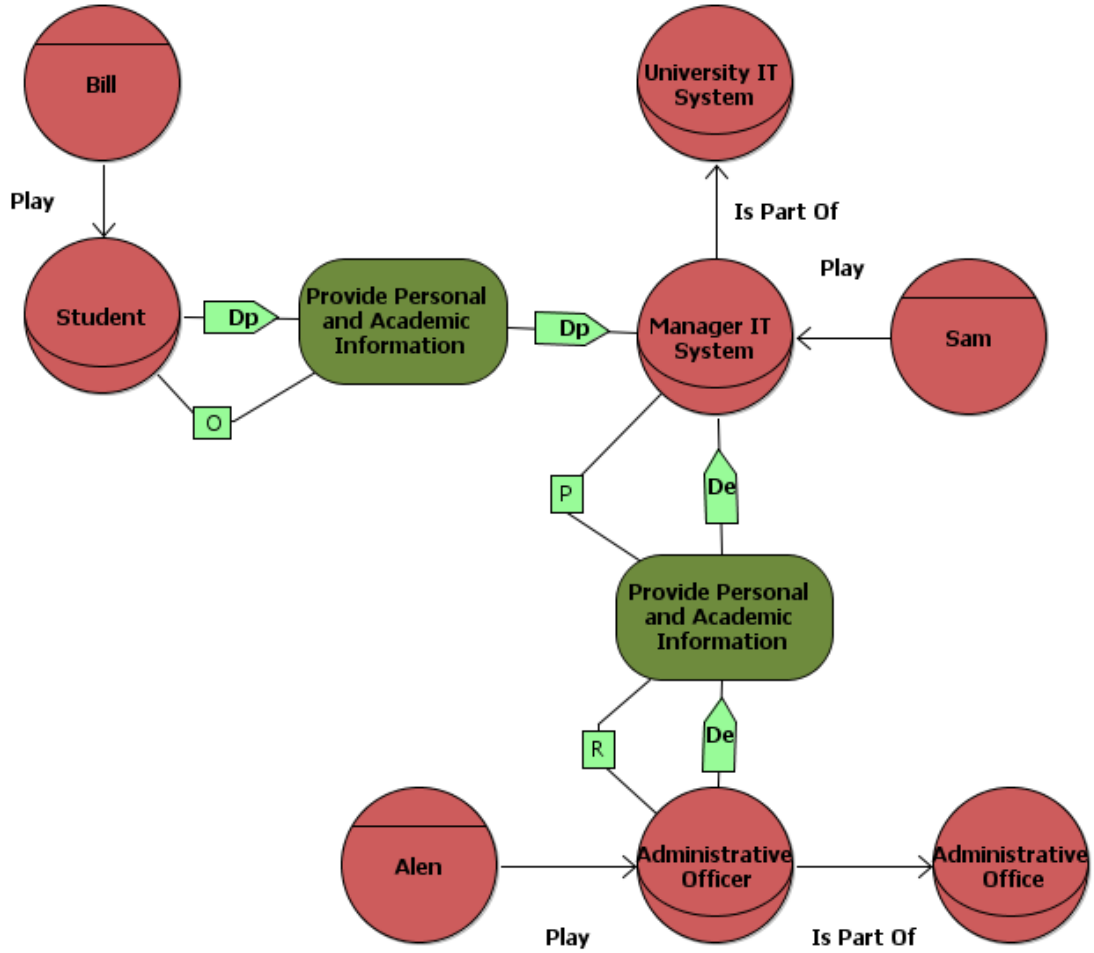

Figure 6.3: Graphical Representation of Delegation Permission of scenario.

Through the *delegation permission* of the goal, now hospital becomes the owner of the goal **Provide Medical Service** and authorized to make any decision to achieve this goal. The main goal of the hospital can be decomposed into sub-goals and for each sub-goal it (hospital) is considered the owner due the transmission of authority of the goal **Provide Medical Service** from Ministry to hospital. For example, the goal of hospital **Provide Medical Service**, can be decomposed into sub-goals **Prescribe Drug to Patient**, **Dispense Drug**, **Generate and Send Drug Reimbursement report** and **Being Reimbursed** and the hospital becomes the owner of all its decomposed goals. It (hospital) can also delegates the

execution of any goal/sub-goals to other actors if it (hospital) is not capable to fulfill them. For example, hospital is not capable to perform the goal **Prescribe Drug to Patient** which is a sub-goal of the main goal **Provide Medical Service**. Hospital appoints doctors and delegates the execution of this goal **Prescribe Drug to Patient** to doctors.

Warning 6.2.1. *Delegating the authority of a service (goal/task/resoucr) to other actor makes the delegator vulnerable. Actually, the delegator has no warranty that the delegatee does not misuse the granted permission.*

6.3 Methodological Steps

This section describes the methodological steps for modeling delegation of authorization of a goal/task/resource using *delegation permission*.

Step 1:

The first step of modeling the delegation of authorization is to identify the actors who transmit or require authorization for performing a goal or executing a task or furnishing a resource. We can analyze the organization structure, business process and business objectives of the organization to find the strategic dependency between actors. Explicitly, we need to identify actors who has the desire to fulfill goals or to execute tasks but delegate the authorization of the goals/tasks to other actors as they do not have the capabilities to ahcieve/execute them. This step also identifies owners(actors) of certains resources who provides the authorization/permission of using their resources to other actors to achieve their goals/tasks. The concept of *Ownership* is very important to model the delegation of authorization. Wheneve any actor B asks for consent to use any service goal/task/resource from another actor A, it is required to check whether actor A is the owner of the service or not. If actor A is the legitimate owner of the service then only he can formally pass the authorization of the service to actor B, otherwise not. This concept of delegation of permission is found in figure 6.4.

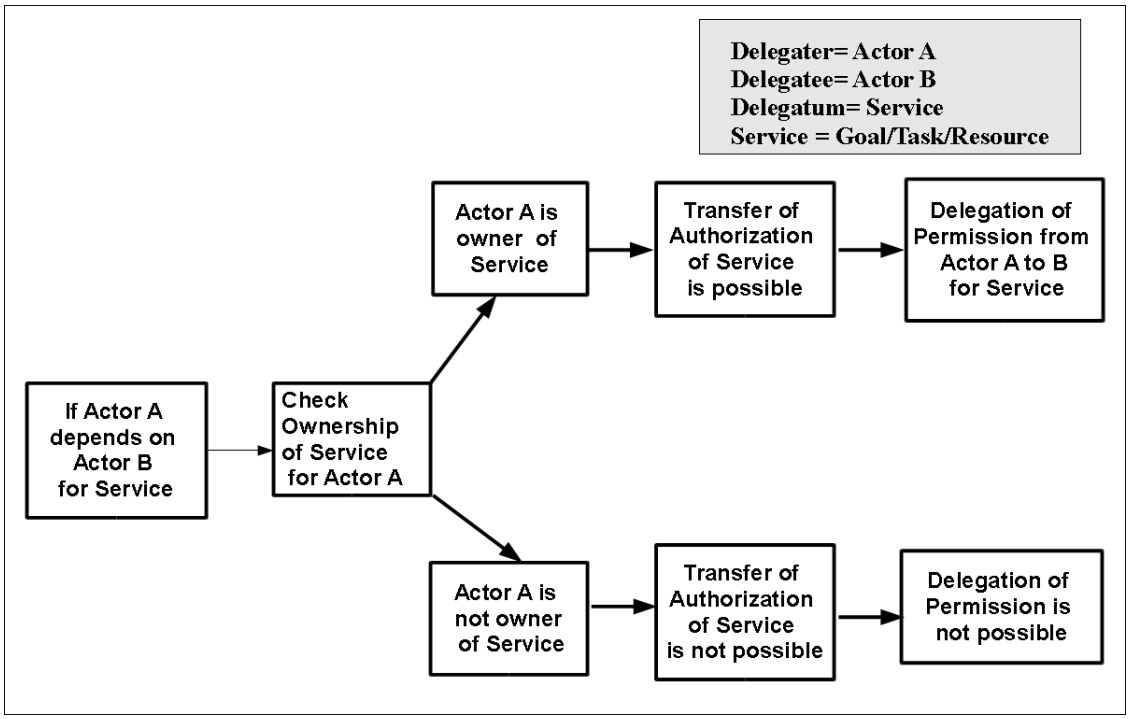

Figure 6.4: Concept of Delegation Permission

Step 3:

After identification of the actors Graphical representation of delegation permission between the actors.

Example 6.3.1. This example focuses on modeling the delegation of authorization of service (goal/task/resource) from one actor to other in the Drug Reimbursement process 1.4. For identifying delegation of authorization among actors in the hospital, we analyze the organizational structure, business objectives and business processes of Drug Reimbursement process 2, 3, 9, 10.

First we search for the actors who have the desire to achieve goals of execute tasks or produce resources but are not efficiency to fulfill their desire. It is found that, the Ministry of Health is the responsible organization to provide healthcare service to patient. As hospital is the skilled organization to accomplish this job, the Ministry delegates the authority of this goal **Provide Medical Service** to hospital. Through this delegation of right of the goal, hospital becomes the owner of the goal **Provide Medical Service** and authorized to make any decision to achieve this goal.

Considering the business processes of Drug Reimbursement process, we also need to find the actors who wait for the approval from the owner of certain resources to use them to acomplish their goals/tasks. We find that, Bob (patient) is the owner of his personal and medical information by law. But hospital requires Bob's (patient) sensitive (personal and medical) inforamtion for administrative and treatment purpose. Particularly, in the drug prescription phase, Alice (doctor) needs to access Bob's (patient) personal information to identify Bob as a patient of Orthopedic unit and his (Bob's) medical record to prescribe him drug. But Alice (doctor) is not entitled to access Bob's (patient) medical record and to fulfill his (Alice) goal he depends on hospital. Hospital seeks permission from Bob (patient) for using his personal and medical information for administrative and treatment purpose. Bob (patient) agrees on hospital's requrest for using his personal and medical data on condition of protecting privacy issue. After obtaining the formal agreement with Bob, hospital gets the right to access Bob's personal and medical information. It allows Alice (doctor) to access Bob's (patient) personal and medical information for fulfilling his goal. Here Bob is the delegator, hospital is the delegatee and Bob's personal and medical information is the delegatum. The graphical representation of delegation permission scenario of Drug Reimbursement process is found in figure 6.5.

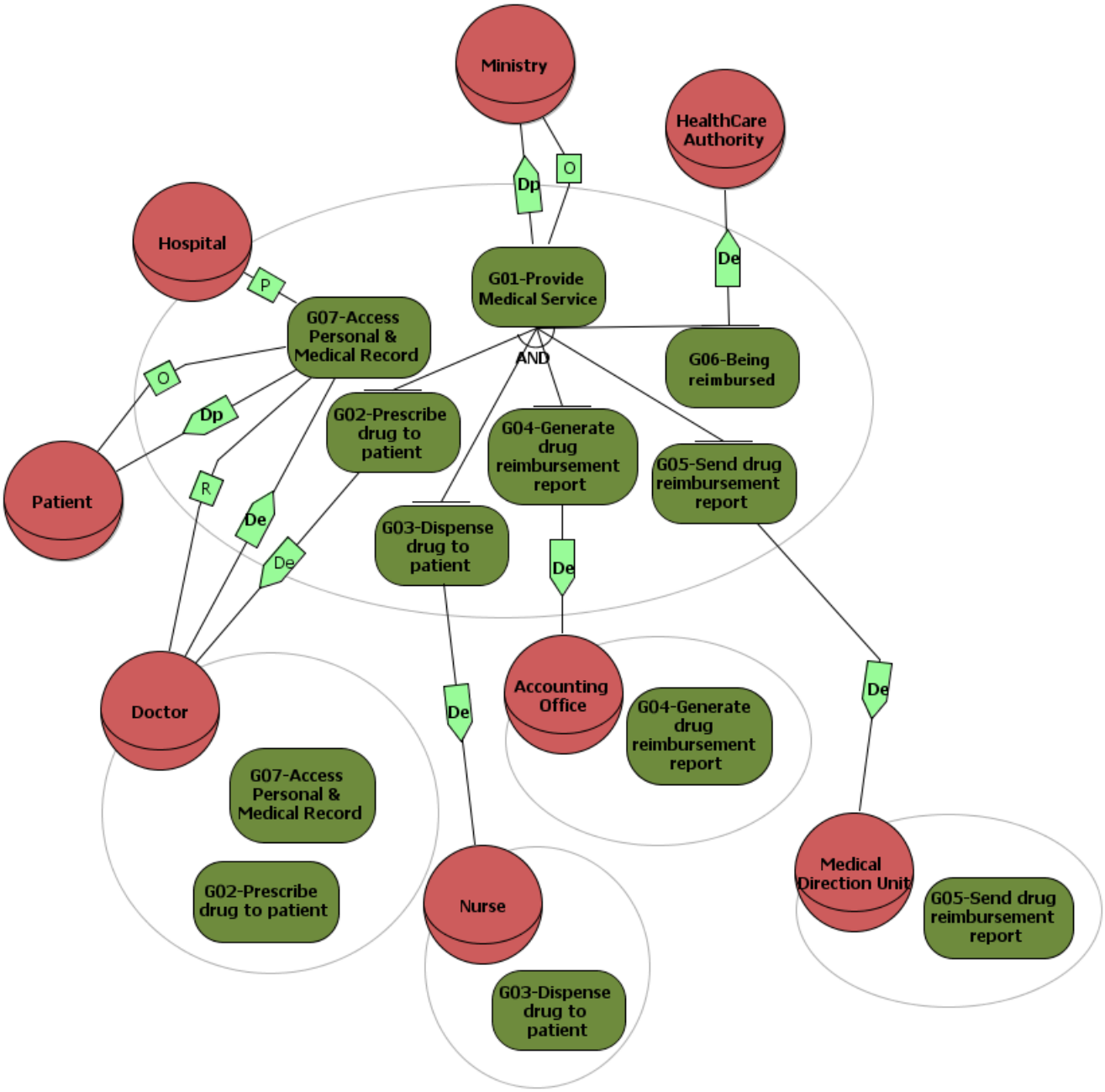

Figure 6.5: Example of Permission Mapping of Drug Reimbursement process.

Chapter 7

Side-Effect Modeling

7.1 Constructs

7.1.1 Contribution Relation

In the organization, business objects (i.e., goals, tasks, resources), events 8.1.1(i.e., uncertain circumstances, threats) and treatments 8.2.4(i.e., tasks to mitigate risks) are related to other business objects by propagating effect due to the success or denial of their occurrence. Modeling these effects (specially negative effect) is very important for the security perspective of the organization.

Example 7.1.1. In the drug reimbursement process described in scenario 1.4, **Archive Prescription sheet** is a goal of doctor in prescription phase. Fulfillment of this goal helps in achieving another goal **Generate Drug Reimbursement Report** in Report Generation Phase by Accounting Office.

Tropos allows capturing this relationship between the business objects in Side-effect modeling using contribution analysis. Typically, contribution is used when the relation between concepts is not the consequence of a deliberative action, but rather results from side-effects. Contribution relations are the most "loose" relations (in terms of the usages) compared to mentioned relations (e.g., decomposition, means-end, needed-by, and dependency) in the Tropos. In nutshell, all relations, except contribution, have nature of causation relation while contribution relations are more similar with the notion of probable causation.

Table 7.1: Predicates of SAT and DEN.

Predicates	Meaning
FS(G)	there is (at least) full evidence that goal G is satisfied
FD(G)	there is (at least) full evidence that goal G is denied
PS(G)	there is (at least) partial evidence that goal G is satisfied
PD(G)	there is (at least) partial evidence that goal G is denied
NS(G)	there is none evidence that goal G is satisfied
ND(G)	there is none evidence that goal G is denied

7.1.2 Satisfaction - SAT and Denial - DEN

For side-effect modeling we need to understand the notion of Evidence adopted from the Dempster-Shafer Theory of Evidence [**?**, **?**], which is similar with the notion of probability. Evidence can be considered as an attribute of Goals, tasks, resources, events 8.1.1(i.e., uncertain circumstances, threats) and treatments 8.2.4 which is refined into two dimensions:

- Satisfaction (SAT)- SAT represents the supporting evidence of the achievement of a goal, the execution of a plan, or the occurrence of an event.
- Denial (DEN) - DEN represents the evidence about the failure in fulfilling a goal, executing a task, or the occurrence of an event.

Though SAT and DEN have similar intuition with probability theory, they are not related and cannot be derived one from the other. The values of attributes are qualitatively represented as Full, Partial, and None, with intended meaning F > P > N. For instance, Sat(G) = P means that there is (at least) partial evidence that goal G will be achieved, whereas Den(G)= N means that there is no evidence about the failure in achieving goal G. Considering the values of the attributes (SAT and DEN) 6 different predicates are shown in table 7.1. Tropos allows us to model the influence/contribution of the satisfaction (or denial) of a business objects (i.e., goals, tasks, resources) to the satisfaction (or denial) of other business objects. This influence/contribution can be positive or negative and is graphically indicated by "+/-" contribution relations. Tropos also has "++" and "- -" to express strong positive contribution and strong negative contribution, respectively. Moreover, to distinguish whether the effect is delivered due the success of a business object, the failure of a business object, or in any cases we add the sign with "S"

(Satisfaction), "D" (Denial), or none respectively. Tropos proposes to use different type of contribution links, namely ++S, +S, - -S, -S, ++D, +D, - -D, -D.

Example 7.1.2. In the drug reimbursement process 1.4, the goal **Archive Prescription, G1** will positively contribute (indicated as G1 $\stackrel{+S}{\rightarrow}$ G2) to the satisfaction of his other goal **Generate Drug Reimbursement report, G2** to patient. Figure 7.1 shows the graphical representation of contribution relation between two goals.

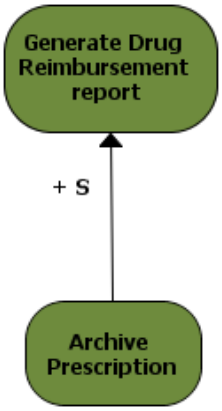

Figure 7.1: Graphical Representation of Contribution relationship.

Warning 7.1.1. *The "sign" positive/negative does not indicate not positive and negative in common sense, but rather indicates the level and the propagation direction of evidence from the source node to the target node. Essentially, +S/++S and -D/- -D are considered as "supporting" contribution (i.e., positive contribution in commonsense), because they add the value of satisfaction evidence to the target node. Conversely, +D/++D and -S/- -S introduce some denial evidence to the target node.*

The semantics of evidence (SAT and DEN) in Tropos is expressed by a set of basic axioms [**?**, **?**] in table 7.2. For simplicity, the notion of Goal (G1, G2 and G3) is used to describe the axioms. The axioms in table 7.2 state that,

- Full satisfiability (or deniability) implies partial satisfiability (or deniability).
- For an "AND" relation, the full and partial satisfiability of the target node (G3) require respectively the full and partial satisfiability of all the source nodes (G1, G2).

Table 7.2: Ground axioms of Evidence(SAT and DEN).

Goal	Invariant Axioms
G	FS(G) → PS(G), FD(G) → PD(G)
Goal Relation	Relation Axioms
(G2,G3) $\overset{AND}{\rightarrow}$ G1	(FS(G2)∩ FS(G3))→ FS(G1) (PS(G2)∩ PS(G3))→ PS(G1) FD(G2)→ FD(G1), FD(G3)→ FD(G1) PD(G2)→ PD(G1), PD(G3)→ PD(G1)
(G2,G3) $\overset{OR}{\rightarrow}$ G1	(FS(G2) ∩ FS(G3))→ FS(G1) (PS(G2) ∩ PS(G3))→ PS(G1) FD(G2)→ FD(G1), FD(G3)→ FD(G1) PD(G2)→ PD(G1), PD(G3)→ PD(G1)
G2 $\overset{++S}{\rightarrow}$ G1	FS(G2)→ FS(G1), PS(G2)→ PS(G1)
G2 $\overset{--S}{\rightarrow}$ G1	FS(G2)→ FD(G1), PS(G2)→ PD(G1)
G2 $\overset{+S}{\rightarrow}$ G1	FS(G2)→ PS(G1), PS(G2)→ PS(G1)
G2 $\overset{-S}{\rightarrow}$ G1	FS(G2)→ PD(G1), PS(G2)→ PD(G1)
G2 $\overset{++D}{\rightarrow}$ G1	FD(G2)→ FD(G1), PD(G2)→ PD(G1)
G2 $\overset{--D}{\rightarrow}$ G1	FD(G2)→ FS(G1), PD(G2)→ PS(G1)
G2 $\overset{+D}{\rightarrow}$ G1	FD(G2)→ PD(G1), PD(G2)→ PD(G1)
G2 $\overset{+D}{\rightarrow}$ G1	FD(G2)→ PS(G1), PD(G2)→ PS(G1)

- For an "OR" relation, the full and partial satisfiability of the target node (G3) require respectively the full and partial satisfiability of any/all the source nodes (G1, G2).

- For a "++S" relation, the axiom states that the achievement of source nodes (G1) can propagate upto full satisfiability for the achievement of target goal (G2).

- For a "+S" relation, the axiom states that the full/partial achievement of source nodes (G1) can propagate only the partial satisfiability (but not the full satisfiability) to target node (G2) through a "+S" relation.

- For a "- -S" relation, the axiom states that the full/partial achievement of source nodes (G1) can propagate the upto full deniability to target node

(G2).

- For a "-S" relation, the axiom states that the full/partial achievement of source nodes (G1) can propagate the partial deniability (but not the full deniability) to target node (G2).

During the contribution analysis, the analysts are concerned about the SAT-related contributions (e.g., +S,-S) as they generally deal with the influence which are passed to the target node only when the source node is achieved. However, there are some situations where the failure in the target node will bring some side effect to another node in a GR model. Such situation is captured by "D" contribution relation which implies the DEN evidence of the resource is propagated to the goal as SAT evidence.

- For a "++D" relation, the axiom states that the failure of source nodes (G1) can propagate upto full deniability for the failure of target goal (G2).
- For a "+D" relation, the axiom states that the full/partial failure of source nodes (G1) can propagate only the partial deniability (but not the full deniability) to target node (G2).
- For a "- -D" relation, the axiom states that the full/partial failure of source nodes (G1) can propagate the upto full satisfiability to target node (G2).
- For a "-D" relation, the axiom states that the full/partial failure of source nodes (G1) can propagate partial satisfiability (but not the full satisfiability) to target node (G2).

Remember 7.1.1. *The propagation of goal satisfaction through a ++S, - -S, +S, -S may or may not be symmetric w.r.t. that of denial. There could be situations where both +S and +D are required for the same goals.*

Remember 7.1.2. *Moreover, (statistical) correlation or conditional probability are other relations that have similar (i.e., not the same) behaviors. For instance, one can see how many ice cream sellers in a beach, then he concludes whether there are sharks or not in the sea. In fact, this does not imply that the ice cream sellers are shark-busters, but rather there is a correlation between two events. In other words, correlation is necessary for a contribution (probable causation), but it is not sufficient.*

7.2 Methodological Steps

Contribution Analysis can be performed after Goal Decomposition 3 and Process Mapping 5 where the main responsibilities of the actors are identified, responsibilities are decomposed into sub-goals and finally tasks and resources are also defined to achieve the goals. The steps of Side-effect modeling are defined in following sub-sections.

7.2.1 Identification of Dependency between business objectives

This phase aims to identify the business objectives (i.e., goals, tasks, resources, events, treatments) which are related to other business objects by propagating effect due to success or denial of their occurrence. We can analysis the actor models, business objectives and business process of the organization to detect the related business objects.

7.2.2 Analysis Contribution relation

This phase aims to analysis the contribution relation between business objects. Here we can model the influence/contribution of the satisfaction (or denial) of a business objects (i.e., goals, tasks, resources) to the satisfaction (or denial) of other business objects.

Example 7.2.1. In this example, we consider the Drug Reimbursement process defined in scenario 1.4. To identify the dependent business objects we analyze the actor model, business objectives and business process of Drug Reimbursement scenario 9, 10. Figure 7.2 shows the Goal Modeling and Process Mapping of Drug Reimbursement process of the hospital where the goals of respective actors are refined and also the tasks/resources required to achieve the goals are identified. We have noticed the following relation in the business objects in Drug Reimbursement process:

- In Drug Prescription phase of Reimbursement process, after patients' identification, doctor of the Operational Unit analyses patient's previous clinical record to prescribe him drug for the current session. So the achievement of

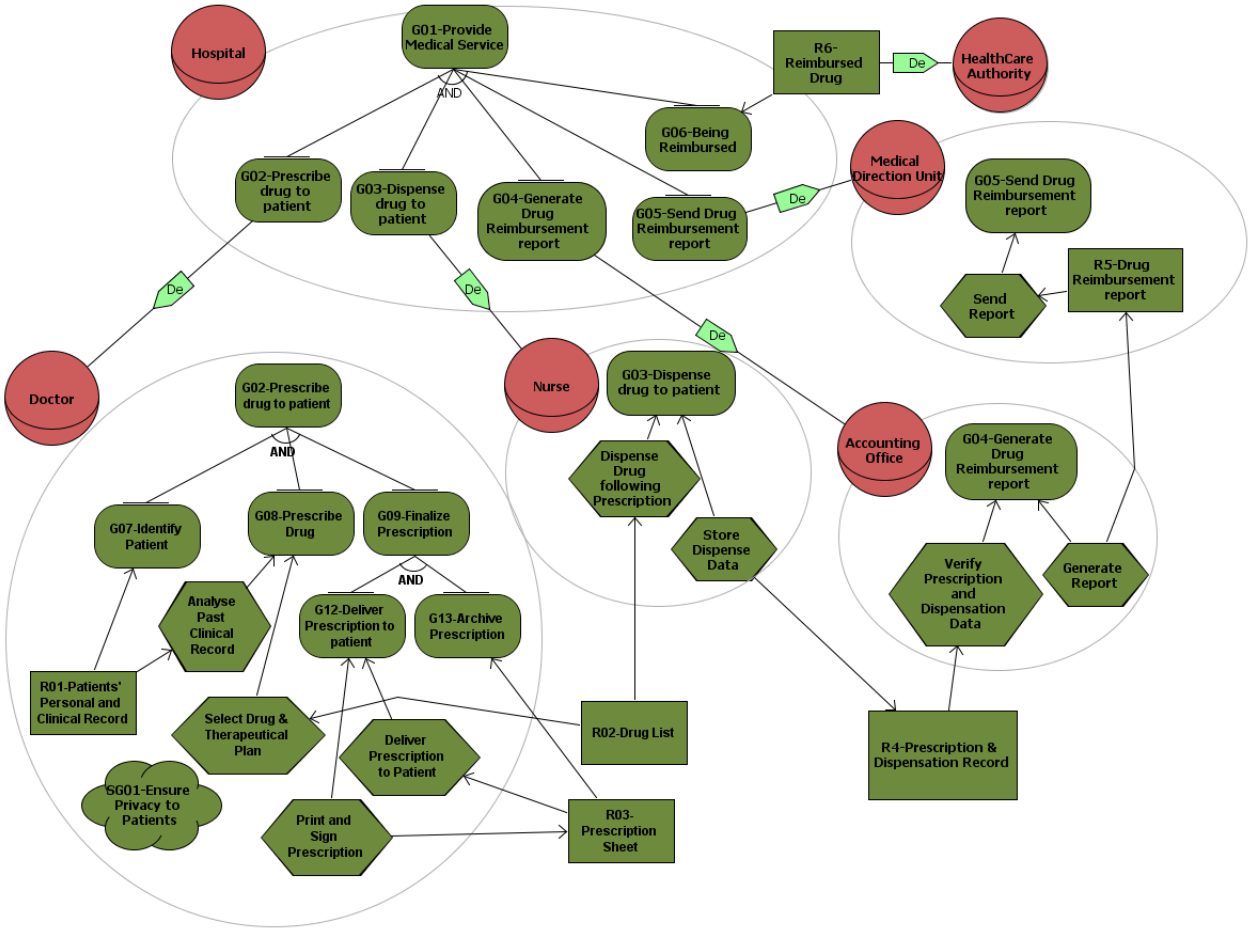

Figure 7.2: Goal Decomposition of Drug Reimbursement Scenario.

goal **Identification of Patient(G07)** can be consider helpful for achieving his other goal **Prescribe Drug (G08)**. So there should be a positive contribution (+S) from goal **Identification of Patient, G06** to goal **Prescribe Drug, G07** as the fulfillment of goal G06 propagates partial satisfiability to the achievement of goal G07.

- In Drug Prescription phase, doctor of Operational Unit analyze the past medical record of patient to understand his medical history. This task **Analyze Patient's Medical Record** is a mean to achieve the goal **Prescribe Drug, G07**. But at the same time, this task **Analyze Patient's Medical Record** hampers **Ensure Privacy to Patients' Info, SG1** which is a soft-goal of Hospital.

- At the end of Drug Prescription and Dispensation phase doctors/nurses archive the prescription and dispensation records for further use. In the Report Generation phase this archived prescription and dispensation record is used for verification and generation of Drug Reimbursement report. So, we find that the goal **Archive Prescription (G13)** and the task **Store Dispensation Data** can be helpful to achieve the task of **Verify Prescribe and Dispensation Data** in the Report Generation phase.

- It is noticed that, achievement of the goal **Send Reimbursement Report (G05)** propagate positive (+S) impact to the fulfillment of the goal **Being Reimbursed (G06)**.

Figure 7.3 shows the side-effect modeling in the goal layer (e.g., between goal, task and resource) of Drug Reimbursement scenario.

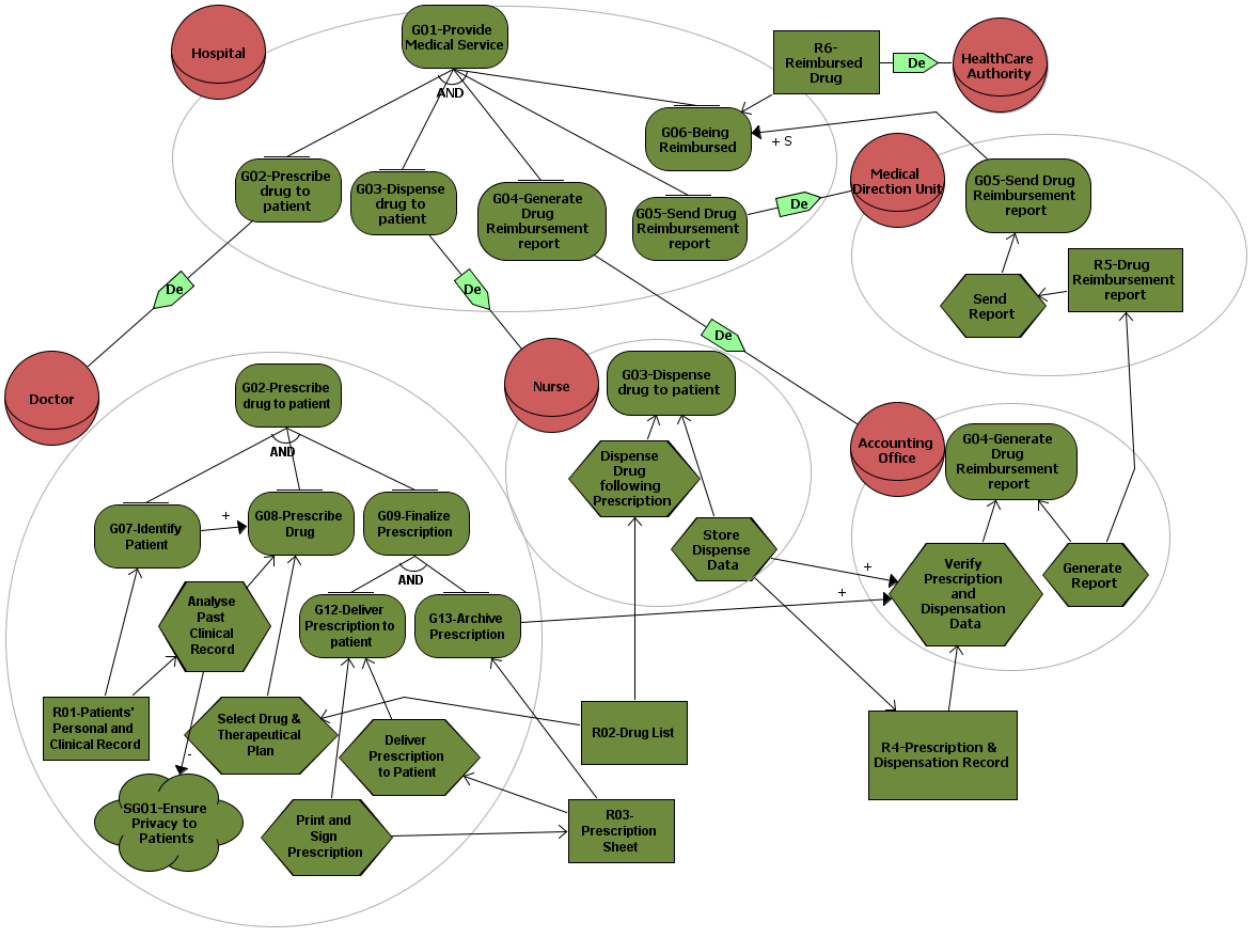

Figure 7.3: Contribution Analysis in Drug Reimbursement Scenario

Chapter 8

Risk Modeling

8.1 Constructs

8.1.1 Event

In organizational environment, uncertain circumstances may arise which are out of control of the stakeholders' and can have an impact (positively or negatively) on the fulfillment of organizations' business objectives.

Example 8.1.1. In Drug Reimbursement process 1.4, **Delay in generating and sending report** to the HealthCare Authority may arise problem in Drug Reimbursement process and obstructs the fulfillment of the goal **Being Reimbursed**. Again, the event **Regular Back-up of Prescription and Dispensation data** may avoid the critical situation which can arises due to the loss or damage of sensitive data of File F system and helps to achieve the goal **Generate and send Drug Reimbursement report**.

The notion of event in Tropos is slightly different from threat in computer security and hazardous condition in reliability engineering. Those concepts defined "event" only as a potential circumstance that could cause harm or loss while Tropos can capture the impact of the circumstance whether it is positive or negative. In Tropos, both the threats against the system and the uncertainties (positive/negative) in the organizations are modeled as events. Tropos characterizes an event as a risk when it produces a negative effect, alternatively an opportunity when it produces positive effects in achieving other business objects (i.e., goals,

tasks, resources). The graphical representation of an event is depicted in 8.1. Tropos characterizes events with two properties:

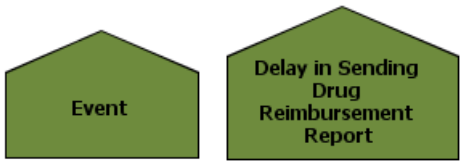

Figure 8.1: Graphical representation of Event.

- **Likelihood** - Likelihood is defined as how likely an event occurs. In Tropos, likelihood of an event is represented by the level of evidence that supports or prevents the occurrence of the event and defined by SAT (satisfaction) and DEN (denial) property 7.1.2. The likelihood is represented qualitatively with the following values: (L)ikely, (O)ccasional, (R)are, and (U)nlikely, with intended meaning L > O > R > U. An event with full evidence of being satisfied and no evidence of denial implies a likely event. Consequently, an event without any evidence of satisfaction results to be an unlikely event, no matter the value of denial evidence.

- **Severity/Impact** - By severity, we mean the influence/impact of an event to the fulfillment of business objects. Tropos supports four levels (i.e., ++, +, - , –) to analyze the impact of an event on business objects:

  Strong Positive (++) - the event occurrence produces a strong contribution to the satisfaction of business objects;

  Positive(+) - the event occurrence produces a fair contribution to the satisfaction of business objects;

  Negative(-) - the event occurrence produces a fair contribution to the denial of business objects;

  Strong Negative(–) - the event occurrence produces a strong contribution to the denial of business objects.

Though the level of evidence of an event can be either supportive (SAT) or preventing (DEN), Tropos concentrates only the SAT value since the effect of an event obstructs a business object only when it occurs.

Example 8.1.2. In Drug Reimbursement process, the occurrence of the event **Delay in generating and sending report** to the HealthCare Authority delivers negative evidence in satisfying the goal **Being Reimbursed** of the Hospital, while the absence of this event does not deliver any evidence neither positive nor negative. Only the occurrence of events can affect the fulfillment of goals and the executions of plans, but their absence do not affect them.

Based on this observation, Tropos assumes that contribution relations from the events propagate only SAT evidences (denoted by ++S, +S, - -S, and -S) to other business objects. Figure 8.2 shows the graphical representation of the impact/influence of an event over a goal where the extent of a contribution relation (positive or negative) is represented by an arrow with + or - sign respectively. Moreover, to represent the evidence which is delivered due the success of a business object, "S" (SAT) is added with the sign.

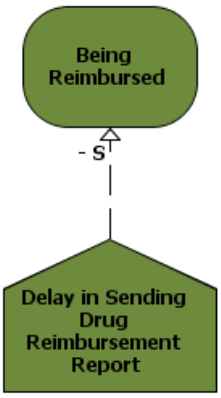

Figure 8.2: Graphical Representation of impact of Event over Goal.

Tropos also allows to model situations where an event can influence more than one goal.

Example 8.1.3. In Drug Reimbursement process 1.4, **Unauthorized access & modification of data** can obstruct the satisfaction of goal **Prescribe Drug** in Prescription phase because in this circumstance doctors will fail to prescribe right drug to the patients. On the other hand, it also can hamper the goal **Dispense Drug** because nurses/doctors will fail to dispense drug due to the unavailability of Operational Unit's drug information.

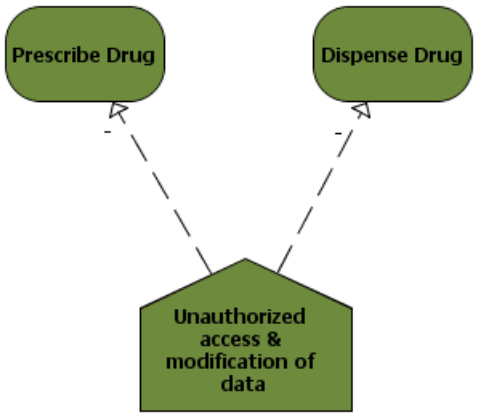

Figure 8.3: Impact of event on multiple goals.

Tropos also provides the flexibility to model an event which acts as a risk and an opportunity at the same time.

Example 8.1.4. In Drug Reimbursement process 1.4, the event **Analyze patients' medical record** can be seen as an opportunity for the goal **Prescribe drug**, because it allows the doctor to understand the patient's current health condition perfectly. However, this event can also be considered as a risk that obstructs the achievement of the soft-goal **Provide privacy to patient** of Hospital.

8.1.2 Risk

Risk can be defined as the events that cause negative effect on achieving the business objectives in the organization.

Example 8.1.5. In Drug Reimbursement process 1.4, the event **Delay in sending Reimbursement report** to the HealthCare Authority can be considered as risk as it may hamper the goal **Being Reimburesd** of the Hospital.

8.2 Methodological Steps

Risk Modeling is very significant in Security and Dependability Tropos as security consideration is the utmost importance in modeling of an organization. Risk Modeling is the continuous process of systematically monitoring, identifying, and analyzing, mitigating risks in an organizational environment. A detail description

of goal-risk modeling is found here [**?**]. Risk modeling steps may introduce new actor as well as new goals, resources and dependencies in the organization. The Risk Modeling steps are described in following subsections.

8.2.1 Step 0: Business Context Definition

The pre-requirement of the Risk Modeling is the Actor Modeling, Goal Modeling and Process Modeling. Before proceed for Risk Modeling, these three modeling steps should perform. Actor Modeling describes in section 2 reveals all the actors and their relationship in the organization. Goal Modeling describes in section 3 deals with the identification of the top level responsibilities of the actors and also the refinement of their responsibilites into lower level. While Process Mapping describes in section 5 maps the required activities to fulfill specific responsibilities of the actor. So after Actor Modeling, Goal Modeling and Process Modeling, it is possible to identify events (Risks) that can hamper an actor to fulfill his goal identified in goal modeling steps.

8.2.2 Step 1: Risk Identification and Refinement

Risk Identification

This step starts with the identification of events that propagate negative impacts on the fulfillment of the business objectives. The identification of the events can be realized using different approaches, such as obstacle analysis [**?**] and anti-goal [**?**]. To avoid confusion in identifying events, [**?**] organises events into three classes-failure, threat and circumstance. Failure is defined as a state where the system delivers a service that is deviated from the requirement. It can occur because of a malicious intent - an attack or just simply an accident. An attack essentially is an executed threat that exploits a particular vulnerability/fault of the system, such as Denial-of-Service Attack where the attack agent has some motivations to bring the service being unavailable and has some method to realize the threat. An accident occurs without any malicious intent where vulnerability is activated by an incident originated from a random process or a human error (e.g., Wrong introduction of Patients' info to File F system). Moreover, risks can also be originated from usual circumstance that is neither failure, threat, nor incident.

Tips 8.2.1. *Availability of assets (or resources) is not sufficient to guarantee the continuity of business objectives. Most of the state of practices defines risks as the obstruction to the availability of some assets. But there could be circumstances where the disruption is introduced from the process or even the objective level. The framework defined in [?] distinguishes risks into three classes and describes the process of risk identification for each class.*

- *Artefact level - To identify risks in artefact level, we can use some taxonomy-base approaches (e.g., computer program flaws, faults) to identify some potential events, or domain-oriented analysis.*

- *Process level - To identify risks at business process management, we need to analyze the business process of the organization to identify the process level risks.*

- *Objective level - The knowledge of works at organization theory, risk at IT governance, and the works on security requirement analysis can be helpful to identify risks at objective level.*

[?] recommends starting the event identification process from the artefact level then move up to the process, and finally the objective level. In this manner, we can prevent the spurious identification of an event's impact. If an event disrupts a resource, then certainly it will also produce a disruption effect to tasks that use such a resource, and consequently this will affect goals that the tasks are supposed to satisfy.

Warning 8.2.1. *An organization can fail in realizing its business objectives due to some circumstance (e.g., new competitors, new regulations, etc.) inspite of the good performance of all the artefacts and business processes. In Drug Prescription scenario, the event* **Reallocation of personnel** *may introduce inconsistency in the organization and may hinder the actors performing their responsibilities. For example, if Alice (Doctor) is recently reallocated from Surgery Unit to Orthopedic Unit but his workstation still contains all information about Surgery Unit instead of Orthopedic Unit then it will obstructs the Drug Prescription phase. In this circumstance, Alice will fail to identify Bob which is a patient of Orthopedic Unit and also will fail to prescribe him drug.*

Warning 8.2.2. *Inappropriate or incomplete identification of risks may lead to failure in achievement of the objectives of the organization.*

Risk Decomposition/Refinement

Identified risks can be refined into lower level. An event is decomposed into sub-events until each leaf event can be easily assessed. Leaf events are used later to find proper countermeasures.

Warning 8.2.3. *Risks should be decomposed into lower level where the sub-risks are disjoint (considered an independent event).*

Risk Assesment

Identified events need to be analyzed along with their influence to the business objects. Moreover, events can also influence the satisfaction or failure of the occurrence of another events which can be modeled using Side-effect modeling 7.2. Tropos assumes that the events propagate only SAT evidences (denoted by ++S, +S, - -S, and -S) to other business objects as the occurrence of events only can affect the fulfillment of other business objects. In the following we describe some situations that could be modeled with Tropos:

- event→ (goal/task/resource): This relation is used to model the impact/influence of risks over the satisfaction of goals, execution of tasks and availability of resources.

  Example 8.2.1. In Drug Reimbursement process, the event **Unauthorized Access & Modification of Data** can obstruct the satisfaction of the goal **Being Reimbursed** of the Hospital.

- (goal/task/resource) → event: These contribution relations are used to model the scenario where a goal/task/resource increases/reduces the occurrence of an event.

  Example 8.2.2. In Drug Reimbursement process, the goal **Archive Prescription Sheet** can reduce the likelihood of the event **Mismatch in Prescription & Dispensation record**.

Table 8.1: Risks in Drug Reimbursement process 1.4.

Risk	Category
Wrong introduction of data to IT system (E01)	Artefact
Unauthorized access and modification of data (E02)	Artefact
Sending Drug Reimbursement report through insecure channel (E09)	Artefact
Lost/Damage of Prescription/Dispensation Data (E07)	Artefact
Incorrect identification of patient (E03)	Process
Mismatch between prescription and dispensation data (E05)	Process
Fake or incomplete Drug Reimbursement report (E06)	Objective
Delay in sending Drug Reimbursement report (E08)	Objective
Reallocation of personnel (E04)	Objective

- event→ event: This relation is used to model dependencies between events/risks where the occurrence of a risk influences/reduces the occurrence of other risks.

  Example 8.2.3. The occurrence of risk/event **Mismatch in Prescription & Dispensation record** can increase the occurrence of another risk/event **Fake/Incomplete Drug Reimbursement Report**.

Example 8.2.4. This example describes the identification, decomposition and assessment of risks of the Drug Reimbursement process described in scenario 1.4. Figure 8.4 shows the goals of Drug Reimbursement process after Goal Modeling 3. It also figures out the resources which are the means to achieve goals. We have followed the guidelines described in [**?**] to identify risks from artefact, process and objective level. Table 8.1 shows the events (risks) that can obstruct actors in the hospital to achieve their goals. We can decompose the top level risks identified in table 8.1 into lower level.

- Unauthorized access and modification of data (E02) - Unauthorized access and modification can occur in patients' medical and personal data, drug

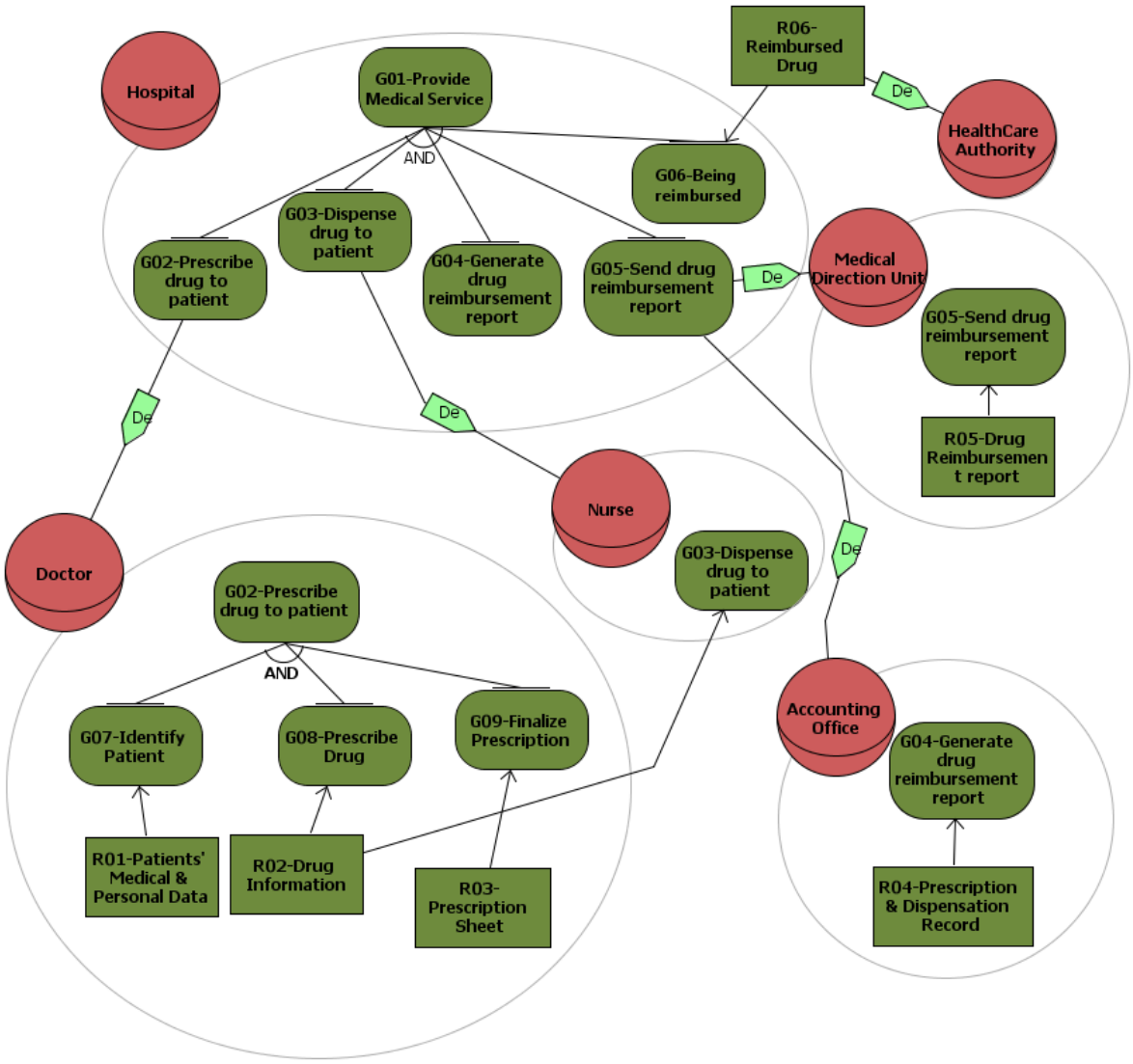

Figure 8.4: Goal Model for hospital in Drug Reimbursement Process.

information, and prescription and dispensation data. So this risk can be decomposed into following four events:

- Unauthorized access and modification of available drug information (E10).
- Unauthorized access and modification of patients' personal and medical data (E11).
- Unauthorized access and modification of prescription data (E12).

  - Unauthorized access and modification of dispensation data (E13).

- Mismatch between prescription and dispensation data (E05)- Mismatch between prescription and dispensation data can occur due to either fake or incomplete prescription/dispensation data. This risk can be decomposed into following risks:

  - Fake prescription or dispensation data (E14).
  - Incomplete prescription or dispensation data (E15)- Prescription/dispensation record is considered incomplete when it is not signed by the doctor or all the fields of prescription/dispensation form are not filled properly. This risk can also occur if prescription sheet is not signed by responsible doctor who prescribed it. So we can decompose this risk into following lower level risks:
    * Unsigned prescription sheet (E16).
    * Prescription sheet is not signed by responsible doctor who prescribed it (E17).
    * Improper/Incomplete fill-up of Prescription/Dispensation form (E18).

After risk decomposition, we have performed the side-effect modeling to model the risks that influence the occurrence of other risks. The dependency between the events needs to be analyzed for this purpose.

- The risk **Unauthorized access and modification of data (E02)** increase the probability of occurrence of the risk **Mismatch between prescription and dispensation data (E05)**, particularly **Unauthorized access and modification of prescription/dispensation data (E12, E13)** increases the chance occurrence of the risk **Fake prescription or dispensation data (E14)**.

- The risk **Mismatch between prescription and dispensation data (E05)** influences the incident of the risk **Delay in Report Generation and Sending (E08)**.

- The risk **Mismatch between prescription and dispensation data (E05)** influence the appearance of the risk **Fake/Incomplete Drug Reimbursement Report (E06)**.

Figure 8.5 shows the risk refinement and side-effect analysis of the risks in drug reimbursement scenario 1.4. Now we need to analyze the impacts of the risks

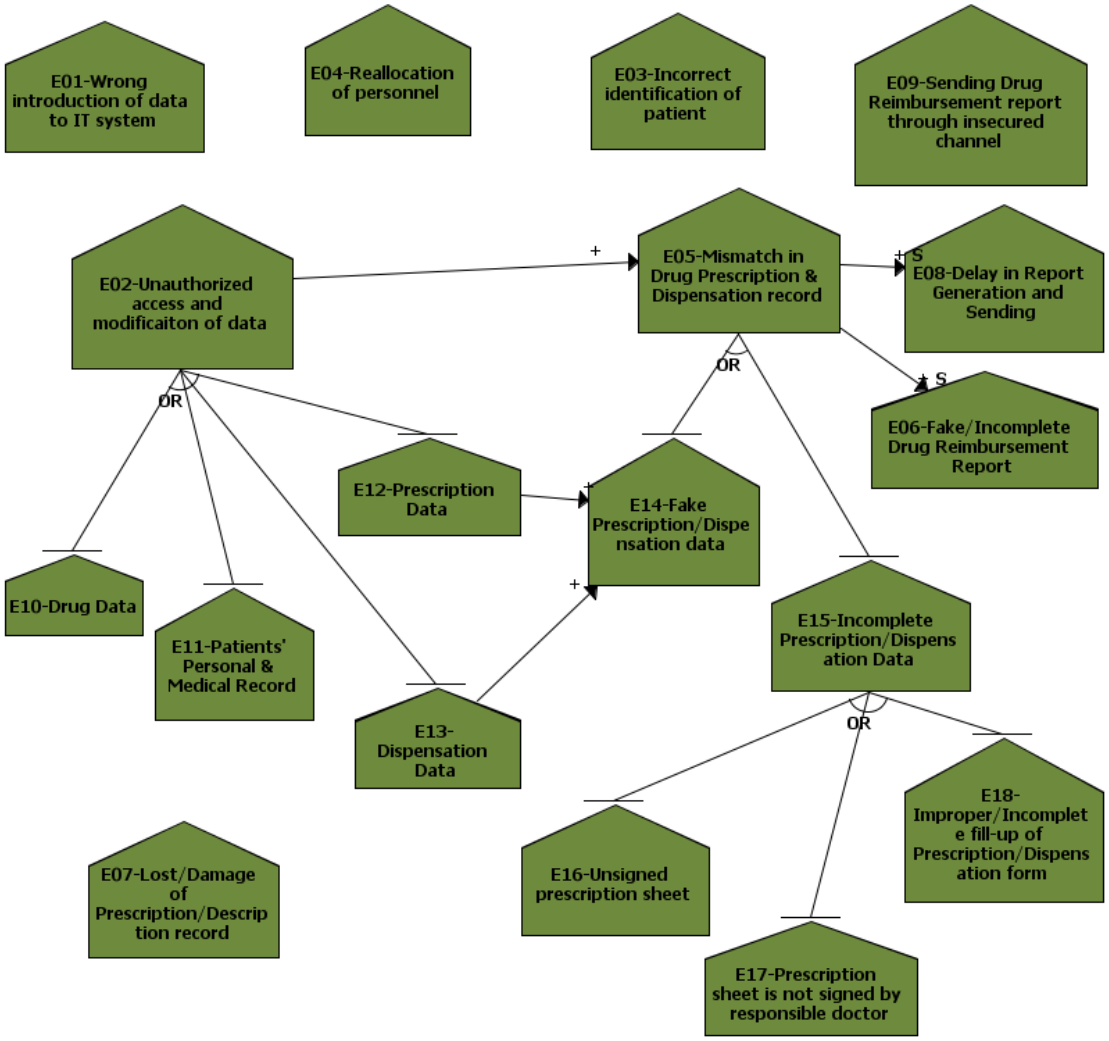

Figure 8.5: Risk Refinement and Contribution relation among risks in Drug Reimbursement Process.

identified on the goal layer defined in figure 8.4. The following events are identified propagating negative impact on the achievement of goals of actors in hospital:

- The risks **Wrong introduction of data to IT system (E01)** and **Reallocation of personnel (E04)** can obstruct the doctor to fulfill his goal of **G07-Identify Patient**. Again, **Unauthorized access and modification of data (E02)** can disturb the availability of the resource **R01-Patients'**

Personal & Medical record and can obstruct the doctor to fulfill his goal of **G07-Identify Patient**.

- The risks **Wrong introduction of data to IT system (E01)** and **Incorrect identification of patient (E03)** may hamper the doctor to achieve the goal **G08-Prescribe Drug**. Moreover, **Unauthorized access and modification of data (E02)** can disturb the availability of the resource **R02-Drug Information** and can obstruct the doctor to fulfill his goal of **G08-Prescribe Drug**.

- The risks **Wrong introduction of data to IT system (E01)** can also disturb the dispensation process. Moreover, **Unauthorized access and modification of data (E02)** can disturb availability of the resource **R02-Drug Information** and can hinder the achievement of goal **G03-Dispense Drug**.

- The events **Mismatch in Prescription & Dispensation record (E05)** and **Lost/Damage of Prescription/Dispensation data (E07)** may arise problem for the Accounting Officer to fulfill his goal **G04-Generate Drug Reimbursement Report**.

- Due to the events of **Use of Insecure Channel in sending report (E09)**, **Delay in Report Generation and Sending (E08)** and **Fake/Incomplete Drug Reimbursement Report (E06)**, HealthCare Authority decides not to reimburse the drug to Hospital. Thus these risks hinder the achievement of the goal **G06-Being Reimbursed**.

Figure 8.6 shows the risks and their impacts on the goal layer.

8.2.3 Step 2: Risk Estimation and Evaluation

This phase is intended to compute the final risk level with defined risk criteria (e.g., cost, benefits, priorities, acceptable loss) and to evaluate whether the risk level is acceptable for the organization. For high level risk, identification of appropriate treatments is necessary to mitigate risks. Risk estimation can be perform by a qualitative and a quantitative reasoner of forward analysis explained in [**?**]. This technique computes the risk level for every actor within an organization and

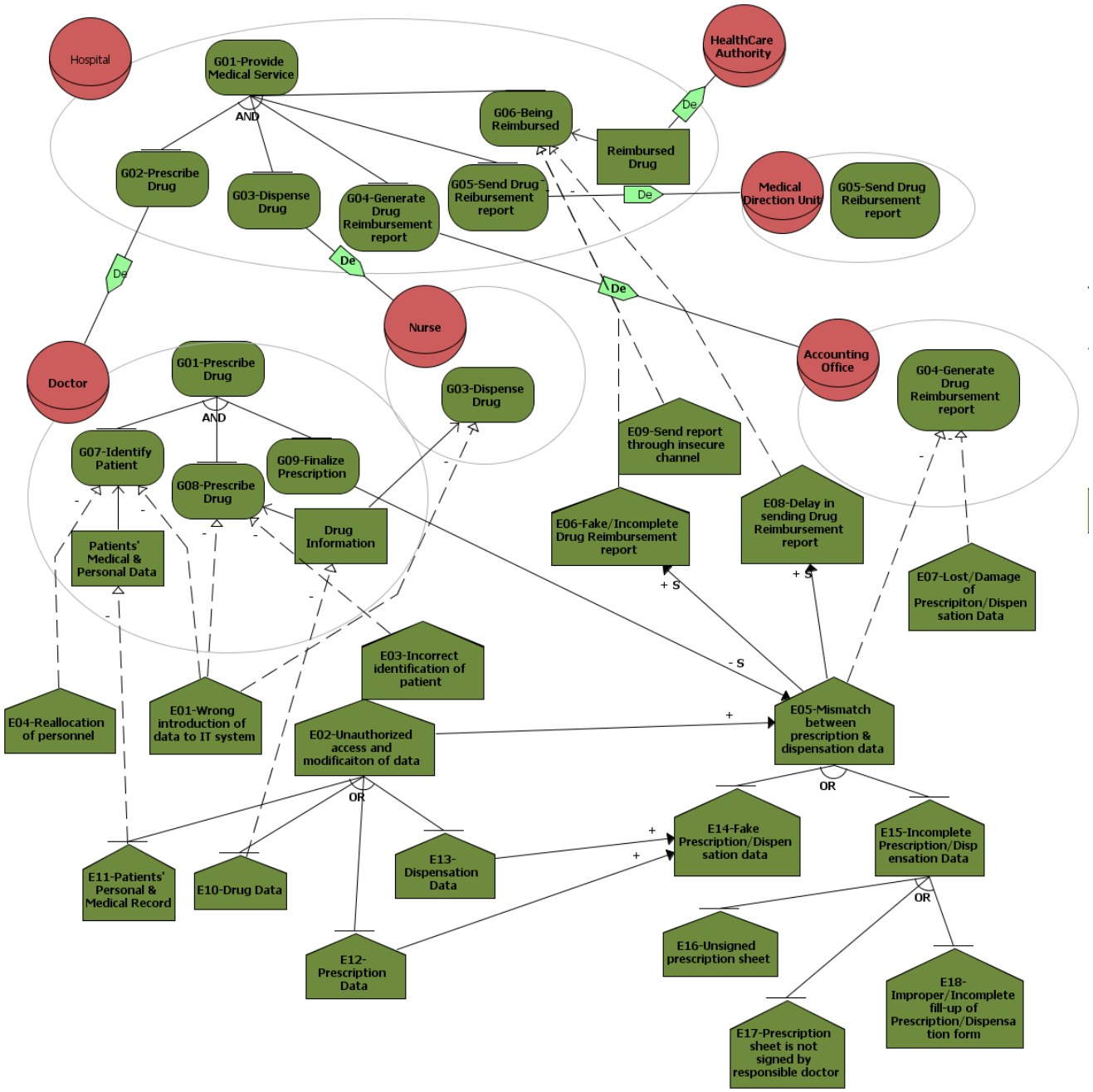

Figure 8.6: Impact of risks on the goal level in Drug Reimbursement Process.

evaluate whether it is within the specific risk tolerance. The risk level for goal G

with respect to actor A can be defined as Loss$\langle\langle A, G\rangle\rangle$ with following equation:

$$Loss\left\langle\langle A, G\rangle\right\rangle = Utility\left\langle\langle A, G\rangle\right\rangle - X_{AG} \tag{8.1}$$

Here, Utility$\langle\langle A, G\rangle\rangle$ is the value specified by the analyst for business goal G with respect to actor A. X_{AG} is the negative evidence of the event for the goal G with respect to actor A. The value of can be calculated through following equation:

$$X_{AG} = \begin{cases} DEN_{AG} + 0.7 \times (1 - SAT_{AG} - DEN_{AG}), if SAT_{AG} + DEN_{AG} \leq 1 \\ DEN_{AG} + 0.3 \times (1 - SAT_{AG} - DEN_{AG}), if SAT_{AG} + DEN_{AG} > 1 \end{cases}$$

In above equation SAT_{AG} and DEN_{AG} are the evidence returned by the forward reasoner. Here the reasoner computes the final SAT and DEN evidence of business goals for a given set of input. For computing the final SAT and DEN value, the reasoner takes the evidence values specified by the analyst for each goal, the utility of a goal with respect to an actor and the likelihood of the events.

The analyst should quantify the evidence values (i.e., SAT and DEN) for each goals, resources, and tasks in the range [0; 1]. Here SAT (or DEN) represents the value of evidence a goal/task/resource will be attained (or be failed) in the future. Each node (goals/resources/tasks) N has two attributes - SAT- Sat(N) and DEN-Den(N) - representing the value of evidence that such node N will be satisfied or denied. It is based on the idea of the Dempster-Shafer (DS) theory of evidence [**?**] where the evidence of a goal (or other constructs) being denied (DEN) cannot be inferred from evidence on the satisfaction of the goal (SAT), and vice versa. The utility of a goal also represents the criticality of a goal for the organization business. It can be denoted in terms of financial unit (e.g., Euro, USD) or just a value in the range [0; 100] according to the priority of the goal.

8.2.4 Step 3: Treatment Analysis

Typically, events are out of an agent's control and the only thing that the agent can do is to try mitigating their impacts. This phase aims at supporting the analyst in evaluating different requirements alternatives with respect to risk. Here we describe the methodological process of introducing countermeasure/treatments to reduce the effect of high level risks.

The first step of Treatment Analysis is to find suitable alternative solutions

together with the actors responsible to execute them to mitigate risks. Then treatments can be either delegated to other actors or refined. During this phase, new actors can be introduced to the system. Afterwards, the effect of treatments mitigating the risks is assessed. Tropos allows to perform cost-benefit analysis over alternative strategies by considering the cost of every strategy besides risks, and adopt the most suitable solution.

Remember 8.2.1. *The treatments are modeled using the same concepts (e.g., task, resource) introduced in Chapter 5. However, the aim of the execution of such tasks or the provision of such resource is not for achieving some goal, but mitigating risks that threaten the system and organisation businesses. In fact, this representation enables the analyst to analysis second order risks (i.e., the risk of treatments) and to ensure the treatments are reliable enough.*

Treatment Identification & Refinement

Identifying treatments are one of the most crucial tasks that analysts must perform to protect the system. To model the reduction of likelihood of risks, we should model a treatment that delivers negative contribution to the risk. Actually, there have been several technologies or techniques are proposed in the literature or the practices to control risks. [**?**] elaborates some guidelines in identifying the most appropriate class of treatment. Particularly it expresses the classes of treatments depending on their behavior:

Avoidance - Avoidance is more an activity than treatment that tries to ensure the attainment of stakeholders' strategic objectives by removing all risk sources (e.g., faults, vulnerabilities, flaws) or selecting no-risk alternatives. In other words, this class is considered more as the principles that one must keep in-mind during system development. Avoidance does not introduce any new additional treatment and/or additional cost to employ-operate treatment. Analysts need to identify some alternatives that are risk-free or an alternative in which they know how to remove (not mitigate) the source of risks. The idea of goal substitution or wakening is considered as a way to avoid risks.

Example 8.2.5. In the drug reimbursement process of File F system described in scenario 1.4, records of prescribed and dispensed drug are the

most important information in generating drug reimbursement report. Possibility of damage of these records can be considered a major risk in reimbursement phase. Analyst can avoid this risk by suggesting the treatment of performing regular back-up of prescription and dispensation record by the IT administrator.

Warning 8.2.4. *Avoidance is not always possible because often risks are introduced because of some business decision, and removing them is considered as ignoring business opportunities. Moreover, often it is impossible to identify all possible vulnerabilities or flaws in the system. Sometimes, avoiding risks is much more costly, than just controlling the risks.*

Prevention - Prevention aims at preventing some negative/bad events to occur in the system. Prevention mechanism operates by propagating i.e., negative-contributions to risks so that the likelihood is acceptable. For using this mechanism, analysts require to identify the entry-point of attacks or the critical state that can lead to failures. Thus, to protect the system from an attack it requires several treatments because it can be originated from several entry points (e.g., outside, untrusted host inside the organization). Moreover, vulnerabilities keep being discovered; hence analysts need to keep employing additional treatments to patch the discovered vulnerabilities. Prevention measures keep operated with/without any presence of attacks or errors, thus they are less cost-efficient to address some rare risks.

Warning 8.2.5. *To prevent the system analysts must define precisely the unit of mitigation from the system that need to be protected as it is hardly possible to protect a whole system. The unit of mitigation of the system is a smaller but very important part of the whole system and requires special attention to secure it.*

Example 8.2.6. In the drug reimbursement process described in scenario 1.4, the achievement of the main business objective **Being Reimbursed** is dependent on the generation of appropriate Drug Reimbursement report. But the Drug reimbursement report generation is mostly dependents on the prescription and dispensation phase where the IT system of File F plays the leading role. The report generation phase may be hampered by unauthorized

access in the IT system of File F and unauthorized modification of prescription and dispensation data. The IT system of File F is vulnerable to attack without suitable security mechanisms and the attacks can be originated from several entry points (e.g., outside, untrusted employees inside the hospital). So the IT system of File F can be done can be considered as the unit of mitigation which requires special prevention mechanisms to be secured. To prevent leaking of sensitive information, an access control mechanisms can be applied in the IT system of File F to limit/control users' access to the sensitive data.

Tips 8.2.2. *Detection mechanisms are highly recommended to be taken as the complementary measures with the prevention. Prevention is good, but detection is necessary because it will protect the system when the prevention fails to prevent an attack. For example: use of access control mechanisms can control the users' access to the sensitive data (prescription, dispensation, patients' information, drug information) to some extent but detection methods are also required to fully protect the system from unauthorized access.*

Detection & Attenuation - Detection mechanism detects the occurrence of risks (e.g., attacks or errors) that cannot be prevented and tries to attenuate them before they compromise the system. Detection operates by suppressing intermediate events (i.e., negative contribution to intermediate or top-level event) or reducing the impact of an event (i.e., alleviation to the impact relation). Moreover, detection is best-suited where there are many entry points to launch an attack, and it only operates at the presence of an attack/error.

Example 8.2.7. In the drug reimbursement process described in scenario 1.4, to mitigate the risk of fraud in generating report of drug reimbursement, Hospital engages Hospital Pharmacy to verify the record of prescribed and dispensed drug by the operational units. The Pharmacy verifies the congruity of the archived record (prescription and dispensation) and sends it back to Accounting Office indicating the errors in the prescription sheets for mitigation.

Tips 8.2.3. *The basic consideration in choosing this class is: detectability of the attack/error and available time to attenuate before it compromises*

the system. In other words, it is not suitable for addressing attacks/hardly that are hardly detectable (e.g., man-in-the middle attack) or has small window time before it manifests as a system failure. Sometimes use of detection mechanisms becomes cost-efficient than applying prevention mechanisms. For example: to mitigate the risk of fraud in credit card, banks prefer to detect bootleg credit cards and revoke them if it is necessary. This countermeasure is far less costly compared with protecting all credit cards from being stolen or copied.

Retention - Finally, a retention works once the risk has succeeded to disrupt the organization, but it tries to make the overall loss is less catastrophic (e.g., insurance, recovery). It is the last alternative to deal with risks. Unlike prevention and detection, analysts do not need to know entry-points/vulnerabilities of the system or possible attacks to retain the system from attacks or failures. Analysts just need to know the existence of deviation for the normal operation in the system, and elicit the measures to recover (or to retain) the system to (up to) the normal operation.

Example 8.2.8. In the drug reimbursement process described in scenario 1.4, Hospital Pharmacy is engaged in checking the congruity of the archived record (prescription and dispensation) to detect the mismatch of information in prescribed and dispensed drug in the Hospital. The Pharmacy verifies the archived record (prescription and dispensation) and sends it back to Accounting Office indicating the errors in the prescription and dispensation data. To mitigate the risk of generation of fake or incomplete drug reimbursement report from the corrupt data, the officer at Accounting Office executes a control query in the system and fixes the error in the archive records. Then this fixed data is used to consolidate the reimbursement database for generating drug reimbursement report. It is noticeable that the Accounting Office is not aiming at detecting and preventing any frauds while they are occurring, but it intends to catch the fraudsters.

Tips 8.2.4. *Retention mechanism operates by supporting business objects to be more robust against risks (i.e., positive contribution to the value layer). Insurance, recovery, and digital forensic are considered as retention measures*

because they do not act against the risks, but more to make the system more retentive in the presence of failure.

Tips 8.2.5. *Essentially, treatments aiming at avoiding risk are done during the system development as they try to avoid the source of risks while the rests aim at controlling risk during the operation of the system.*

Tips 8.2.6. *Though analysts have employed prevention and detection, sometimes it is necessary to adopt some recovery or retention measures because new vulnerabilities and attacks are being discovered or invented. Moreover, analysts ideally employ several controls from difference classless for an critical business object (i.e., security in-depth principle). For example: in the drug reimbursement process of File F system 1.4, to prevent the risk of generating fake or incomplete drug reimbursement report, Hospital employs prevention measures (e.g., access control mechanisms) that limit the access of the sensitive information (prescription and dispensation data) by attacker. However, the hospital still engages Pharmacy for the detection of anomalies in archived information. The Pharmacy informs the Accounting Office about the errors in the data and finally the Officer of Accounting Office tries to fix the errors.*

Treatment Assessment

This phase aims at assessing the effect/influence of treatments to mitigate risks. A treatment may affect on a risk in two different ways: reducing its likelihood or attenuating its severity. To reduce the likelihood, a treatment is modeled using a contribution relation which introduces denial evidence to the event; and to reduce the severity, it is modeled using an alleviation relation. In Drug Reimbursement scenario 1.4, the treatment **Ensure timely delivery of Drug Reimbursement report** can apply to alleviate the impact of the risk **Delay in Report Generation** 8.7. Similarly to goals and events, for treatments we use SAT and DEN 7.1 to represent the evidence that supports and prevents the action. We represent the effect of a treatment over risks as a relation, where its strength is expressed by the sign of the contribution relations 7.1.1. As treatments/countermeasures are introduced particularly to mitigate the risk, we are interested to the propagation of the evidence for the success of a treatment (SAT).

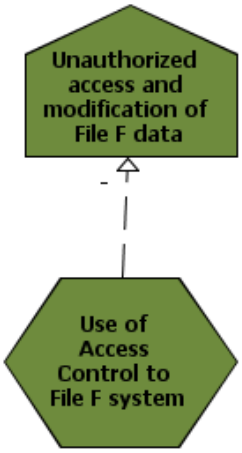

Figure 8.7: Modeling treatment using alleviation relation.

Example 8.2.9. This example describes the treatment identification and assessment of drug reimbursement process defined in scenario1.4.

- The doctor needs to **Ensure correct patients' identification (T01)** to reduce the risk of **Incorrect identification of patient (E03)**. He also needs to **Ensure correct & complete fill-up of the prescription form (T02)** and **Avoid signing prescription prescribed by other doctor T03** to avoid the occurrence of the event **Incomplete Prescription/Dispensation Data (E15)**.

- In the dispensation phase, the nurses/doctors should be careful and **Ensure correct & complete fill-up of the dispensation form (T02)** to avoid the occurrence of the event **Incomplete Prescription/Dispensation Data (E15)**.

- The identification of treatments introduces two new actors to model which are IT Office and Hospital Pharmacy. Though the main goal of IT office is to maintain the File F system, but here to mitigate some risks in Drug Reimbursement process, it also needs to perform some tasks. The IT office can introduce **Access Control for File F system (T08)** to avoid the risk of **Unauthorized access and modification of data (E02)**. It needs to make Regular Back-up of Prescription and Dispensation Data (T07) to avoid the problem due to **Lost/Damage of Prescription/Dispensation**

Data (E07). Careful data entry in File F system (T10) should be another task of the IT office to reduce the risk of **Wrong introduction of data to IT system (E01)** and **Ensure required changes in File system with reallocation of personnel (T11)** can evade the risk occur due to **Reallocation of personnel (E04)**. Hospital Pharmacy also needs to perform a significant task to help the hospital being reimbursed. The pharmacy can **Detect error in Drug Reimbursement record (T9)** by checking the prescription and dispensation record to avoid the event **Mismatch between prescription & dispensation data (E05)**.

- The Accounting Office needs to do **Correction of errors in Drug Reimbursement Record (T04)** to mitigate the risk and it also need to **Ensure timely delivery of Drug Reimbursement report (T05)** to avoid the risk of **Delay in sending Drug Reimbursement report (E08)**.
- The Medical Direction Unit should **Use of secure channel for sending report (T06)**.

To mitigate the risks of drug reimbursement process, the following treatments in table 8.2 are identified with the responsible actor. Figure 8.8 shows the treatments to mitigate the risks identified Reimbursement scenario 1.4.

There may be a situation where treatments/countermeasures also effect to achieve a goal, to execute a task or to availability of a resource. Countermeasures/treatments can also effect (positively or negatively) in occurrence of other treatments. Tropos allows to model situations through Side-effect modeling 7.2 where a treatment/countermeasure adopted to mitigate a risk has also a contribution (especially negative) to some other business objects (e.g., goals, tasks, resources, treatments).

Example 8.2.10. In the drug reimbursement process 1.4, the treatment Ensure Regular Back-up of Prescription and Dispensation Data (T07) is introduced to avoid the problem due to **Lost/Damage of Prescription/Dispensation Data (E07)**. But this treatment can deliver negative contribution to achieve the main goal of IT office **Maintain File F system's operation**, because the IT office, now, has a new task and consequently it results in the IT office having a smaller capacity to control File F system than before.

Table 8.2: Treatment Identification to mitigate risks in Drug Reimbursement process 1.4.

Treatment	Actor
Ensure correct patients' identification (T01)	Doctor
Ensure correct & complete fill-up of the prescription and dispensation form (T02)	Doctor, Nurse
Avoid signing prescription prescribed by other doctor (T03)	Doctor
Correction of errors in Drug Reimbursement Record (T04)	Accounting Office
Ensure timely delivery of Drug Reimbursement report (T05)	Accounting Office
Use of secure channel for sending Drug Reimbursement report (T06)	Medical Direction Unit
Regular Back-up of Prescription and Dispensation Data (T07)	IT officer
Use of Access Control for File F system (T08)	IT officer
Detect error in Drug Reimbursement record (T9)	Hospital Pharmacy
Careful data entry in File F system (T10)	IT officer
Ensure required changes in File system with reallocation of personnel (T11)	IT officer

Treatment Analysis & Adoption

This phase describes the cost-benefit analysis of treatments and adoption of suitable treatments. However, analysts should not base their decision only with the value of "cost-benefit" (i.e., ratio), because the most beneficial alternative might introduce some side-effects that are unacceptable.

Remember 8.2.2. *Analysts thus can negotiate a solution with the actors even if residual risk is higher than risk tolerance due to the cost of treatments. When actors cannot accept the residual risk, analysts need to identify additional treatments until the residual risk is acceptable. Often the selected treatments are not sufficient to mitigate risks. Therefore, stakeholders may decide to accept the risks.*

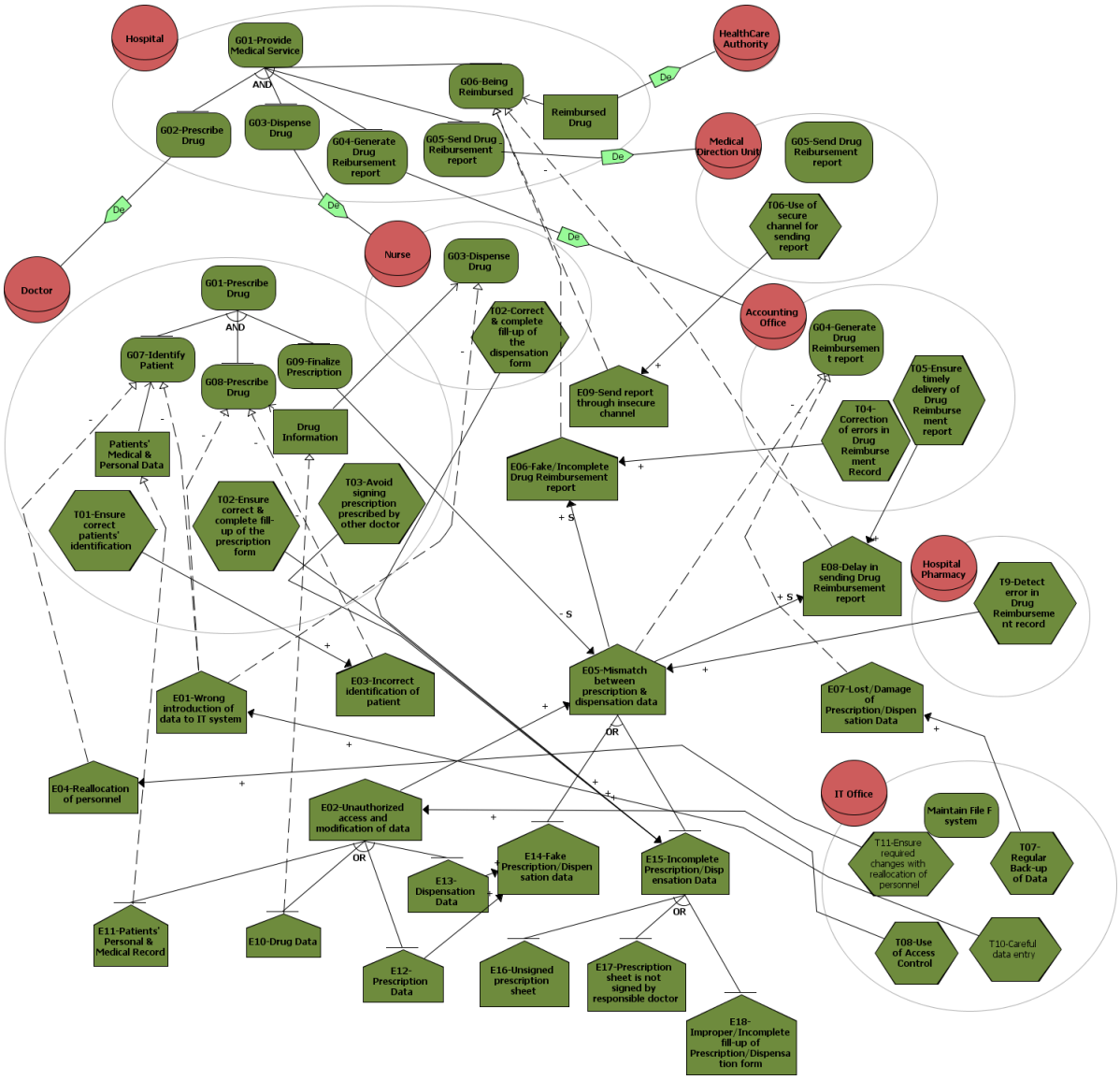

Figure 8.8: Risk Modeling of Drug Reimbursement scenario.

Chapter 9

Appendix A

Abstract

The Drug Prescription is the first phase of Drug Reimbursement process. The prescription is done by the doctors to the patients using an IT System. The doctors retrieve all the previous medical records of the patients using the IT System and choose the drugs to prescribe in the current session by considering the past medical records.

9.1 Introduction

9.1.1 Drug Reimbursement

In Italy, the outpatient drug reimbursement is regulated by the Ministry of Regional government. The Ministry dictates the regulations and guidelines for reporting reimbursable drugs to Regional Directorate through standard files and a standard process called Drug Reimbursement of File F. The Drug Reimbursement process is composed into four phases:

P1 : Drug Prescription

P2 : Drug Dispensation

P3 : Generation of File F report

P4 : Send File F report

Phase P1 and P2 are performed daily for each treatment to a patient, and P3 and P4 are performed monthly to prepare and send the File F report to the Healthcare Authority for the drug reimbursement. This case study emphasises on the drug prescription phase, and describes in detail the business objectives, business processes, assets, actors and risks of this phase.

9.1.2 Drug Prescription Phase

Prescription phase is executed by the doctors and the patients through the Prescription module of the IT System of the hospital. First the doctor has to identify the patient in order to give a prescription. Doctor retrieves all the past medical record of the patient from the IT System. The doctor needs to consider her/his previous medical reports in giving the prescription. A prescription is the health-care program for the patient which includes the name of the drug items, posology and quantity. Finally, doctor prints the prescription and gives the signed prescription sheet to the patient.

9.2 Business Objectives

- Prescribe the right drugs to the right patient with specific therapeutic plan (drug quantity, posology).
- Provide privacy to the patient by giving the opportunity of being pre-scribed as anonymous.
- Populate Clinical Record/Prescription and input for the dispensation phase with respect to Drug Reimbursement regulation.

9.3 Actors

This phase involves several actors and each has its own goal as described in the Table 9.1.

Figure 9.1 shows the actor Model of the prescription phase. Hospital includes Operational Unit where the doctors are associated with the Operational Unit. HealthCare Authority supervises the hospital to follow the healthcare regulation.

Actor	Responsibility
Hospital	Provide Health-Care Service
Doctor	Provide right prescription to patient
Patient	Get Prescription with appropriate drug and therapeutical plan
Operational Unit	Monitor and Handle drug stock and patient data.
Healthcare Authority	Monitor and analysis Drug Reimbursement report collected from hospital

Table 9.1: Actors' Responsibility in the Prescription Phase

Figure 9.2 shows the dependency relationship between the actors in prescription phase. Patient depends on the doctor for getting the prescription. Doctor depends on the Operational Unit for getting the patient's data and the drug list associated with the Operational Unit to identify the patient and suggest drug. HelathCare Authority depends on the Hospital for profiling the prescription sheet which is considered as the Clinical Record.

9.4 Regulatory Compliance

Regulatory Reference Italian Legislative Decree No. 196/2003 "Personal Data Protection Code": this law indicates the "Technical Specifications Concerning Minimum Security Measures" to apply to data processing done by electronic means. In particular in Annex B are specified the requirements about the "Computerized Authentication System", the "Authorization System", the "Security Policy Document", the "Additional Measures Applying to Processing of Sensitive or Judicial Data", etc. According to this regulation Hospital needs to protect sensitive or judicial data against unauthorised access by implementing suitable electronic means.the Regulatory requirement of the prescription phase is the requisition for anonymity of patients' data records where the request for anonymity is done by the patient. This requirement was placed especially because of the character of the respective diagnoses, where for instance belong those with sensitivity and Privacy protection.

Regulatory Reference Regional Circular No.5/SAN 30-1-2004 (and followings Circulars)] indicate the guidelines for sending Drug Reimbursement report

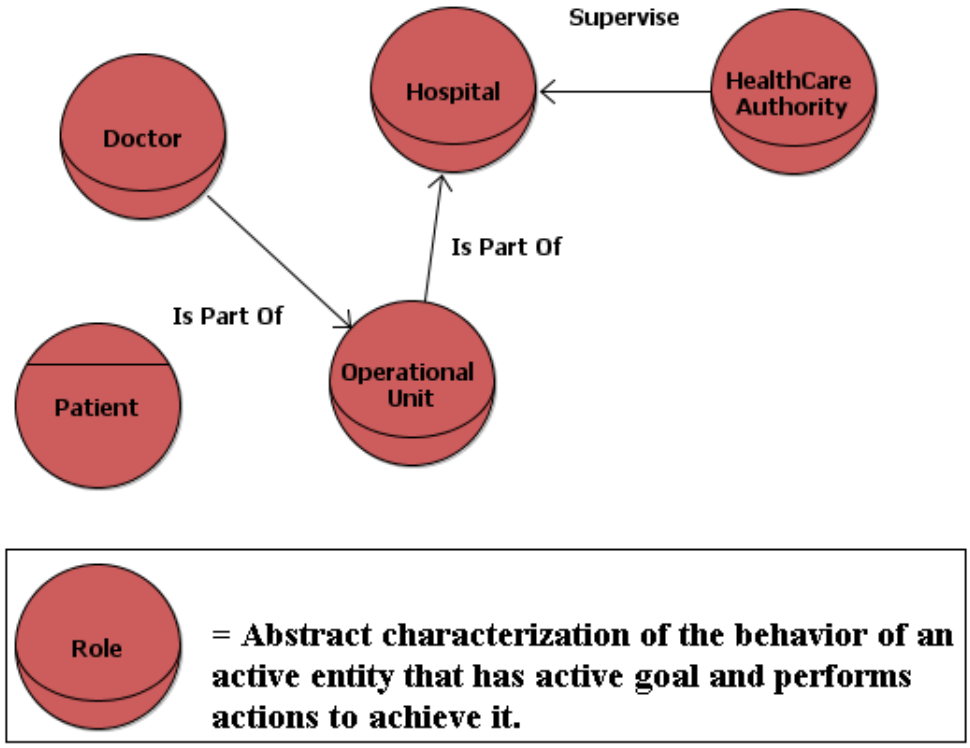

Figure 9.1: Actor diagram of the Prescription phase.

to Healthcare Authority. According to these regulations the Hospital has to produce the File F reports (FF1, FF2, FF3) including all the data required (personal data, data about drugs, etc.). moreover this regulation institutes the "debito informativo" channel to send the reports to the Authority (certified e-mail using cryptographic methods).

9.4.1 Reference indicating best practice

Reference "Governance, Leadership, and Direction" GLD.2 defined in Joint Commission Accreditation indicates the best practice where in Hospital a senior manager or director is responsible for operating the organization and complying with applicable laws and regulations.

Reference MCI.10 defined in Joint Commission Accreditation indicates the best practice for "Management of Communication and Information". Refer-

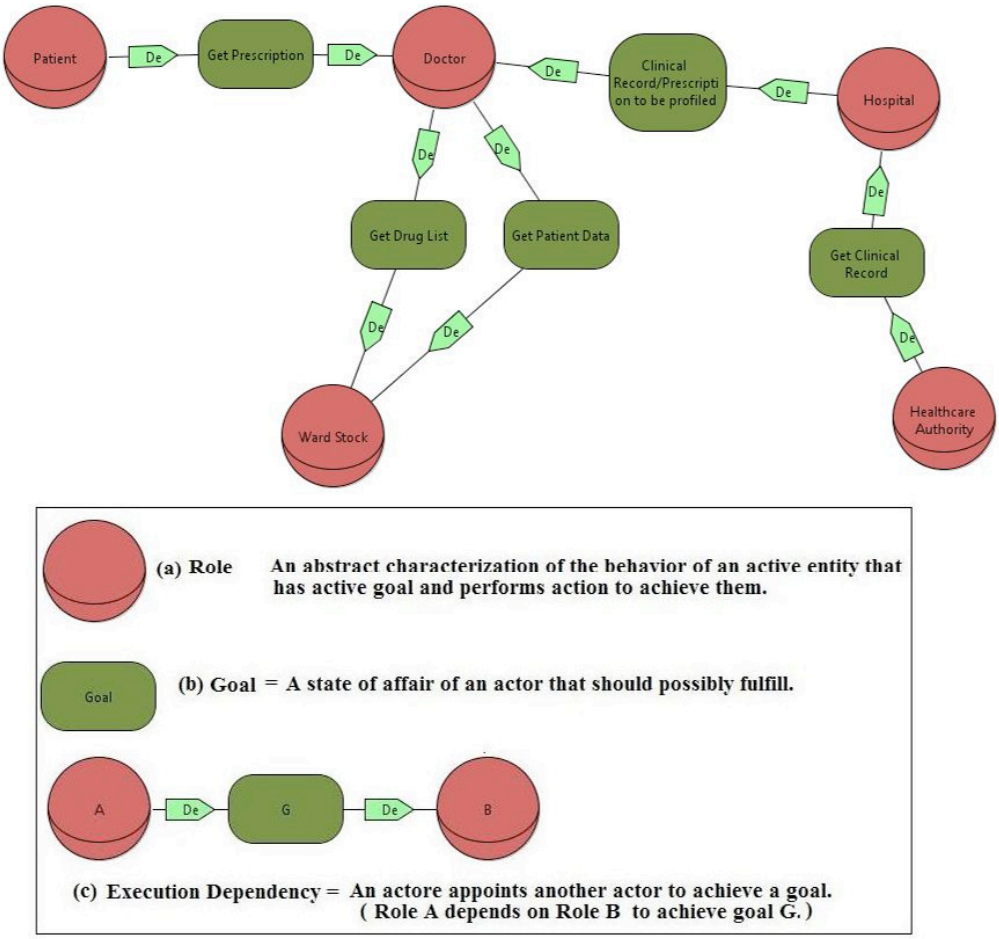

Figure 9.2: Prescription Phase of Drug Reimbursement.

ence MCI.10 indicates best practice for maintaining Information privacy and Confidentiality, reference MCI.11 indicates practice for maintaining Information security including data Integrity. MCI.18 reference defines protocol stating the requirements for developing and maintaining policies and procedures.

9.5 Assets

The hard assets of prescription phase are defined below:

Drug The stock of drug in the operational unit.

Drug Data The information of the drug stored in the operational unit.

Patients data Information of the patients who are associated with specific operational unit.

The assets can be described as follows:

1. Document
    - Prescription Sheet : The outcome of the prescription phase. The prescription is the printed health-care program prescribed and signed by the doctor.
2. Data
    - Drug Data : Information of the drugs in the operational unit. Drug data contains: name, type, and price.
    - Patient Data : The patient data indicates both personal and medical data. The personal data includes the Identification code (Tax code), Name and Address. The medical data includes:
        - Historical Diagnosis and Treatment
        - Previous prescription
        - Previous dispensed drug list
    - Personnel (Doctors) Data : This includes the doctors data who are associated with specific ward stock in a department within the hospital.
    - Prescription Data : Prescription defines the health-care program suggested by the doctor. The main information that the prescription sheet contains: Drug Name, type, quantity, and Posology (Therapeutical Coverage)

9.6 Analysis of business processes

The main business objective of the drug prescription phase is to generate right prescription for right patient. So the main business process of the drug prescription is generation of the prescription. Figure 9.3 shows the business process of drug prescription phase. The process starts when any patient needs the treatment. The doctor tries to identify the patient in order to assign a prescription. The IT system

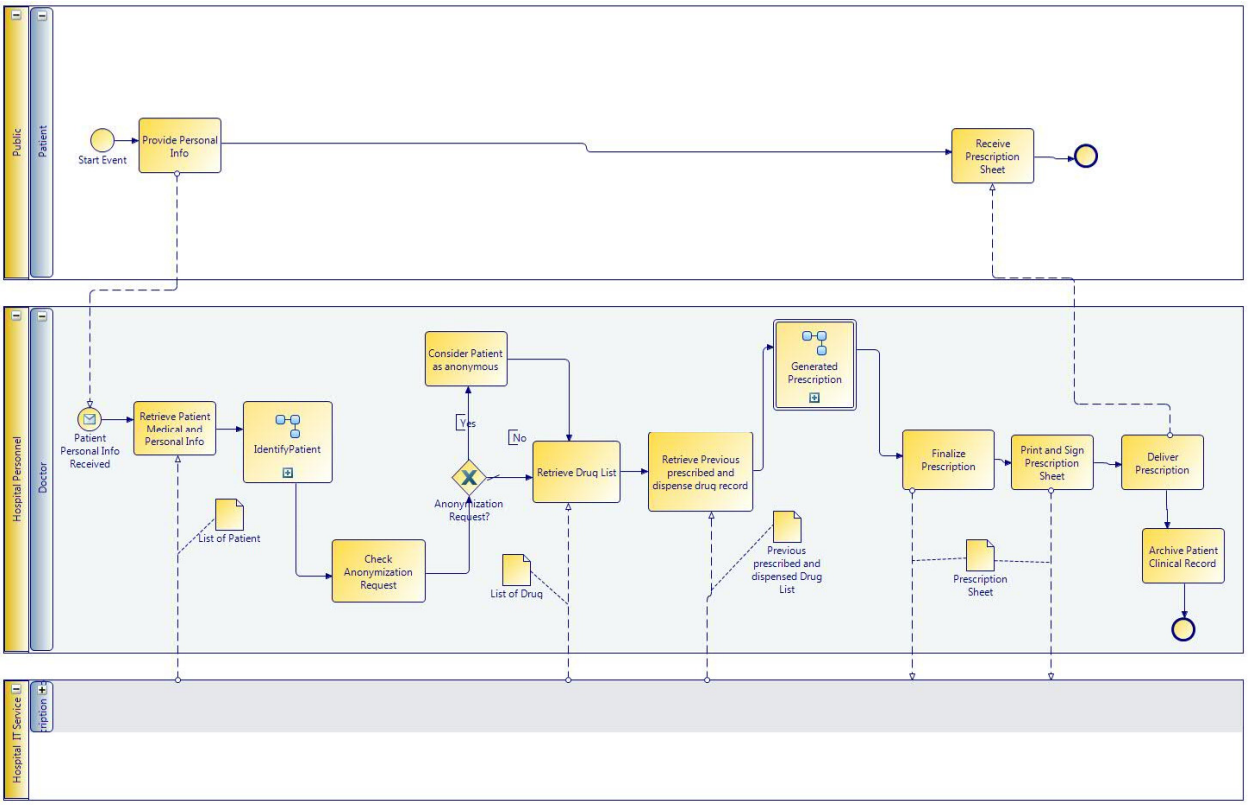

Figure 9.3: Business process of Prescription Phase.

retrieves all the record of the patient including personal and medical data in the prescription phase. The patient identification is defined in sub-process in Figure 9.4.

The patient identification can be done by patient identification number. In order to identify the patient, the doctor can give input any identification information of the patient in the system such as the Tax code, STP code, Team code or the Clinical record code.

Another business objective is to provide privacy to the patient by giving the opportunity of getting treatment as being anonymous. So in the business process after patient identification, the patient will be prescribed as anonymous if he requests for that.

Then the system also retrieves all the previously prescribed or dispensed drugs to this specific patient. After the patient identification the doctor can proceed for the generation of prescription. This is given in Figure 9.5 the generation of

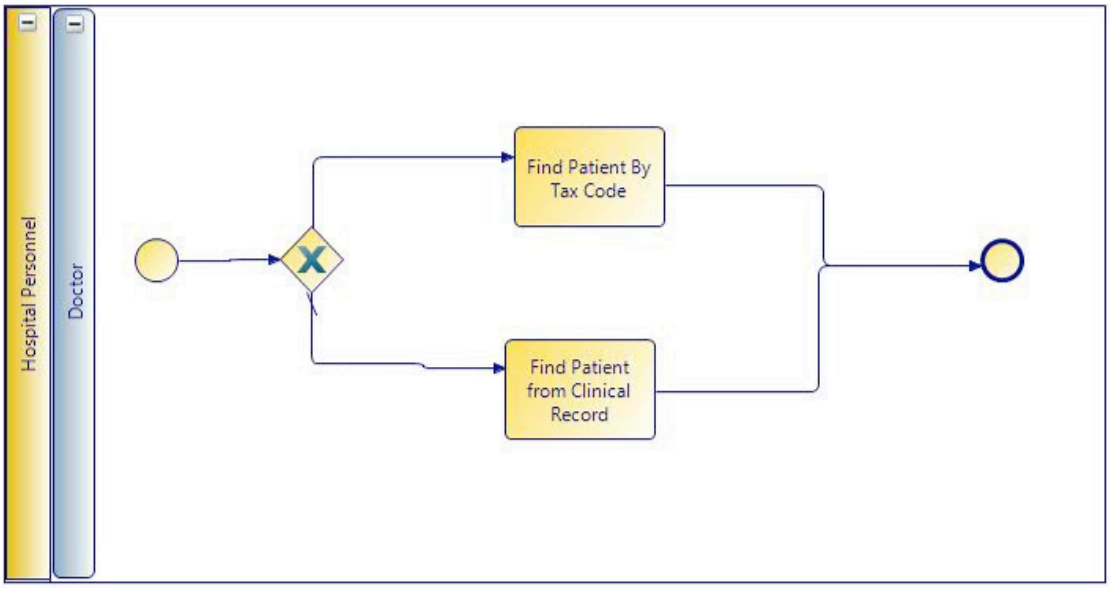

Figure 9.4: Patient Identification sub-process.

prescription sub-process. The doctor analyses the diagnosis reports of the patient and the previous prescribed and dispensed drug list. Then he selects the drug and the drug selection can be done from the drug list of the ward stock with which the doctor is associated. The doctor can also select drugs from the list of the drugs previously prescribed or from the list of the drugs previously dispensed.

Finally the doctor has to register the prescription data. Before the registration confirmation, the doctor can modify or delete the prescription information. Then the prescription is printed and the doctor has to sign the sheet and give the sheet to the patient. The prescription phase ends by archiving the prescription of the patient as clinical record to send to the Regional Authority.

9.7 Risk of Drug Prescription Phase

1. Re-allocation of the personnel may hampers the prescription phase because it may occur inconsistency between the operational unit from where doctor is prescribing the drug with the actual operation unit the doctor is associated with.

2. Drug reimbursement report can be generated using false prescription (prescription that is not prescribed) record. This hampers the drug reimburse-

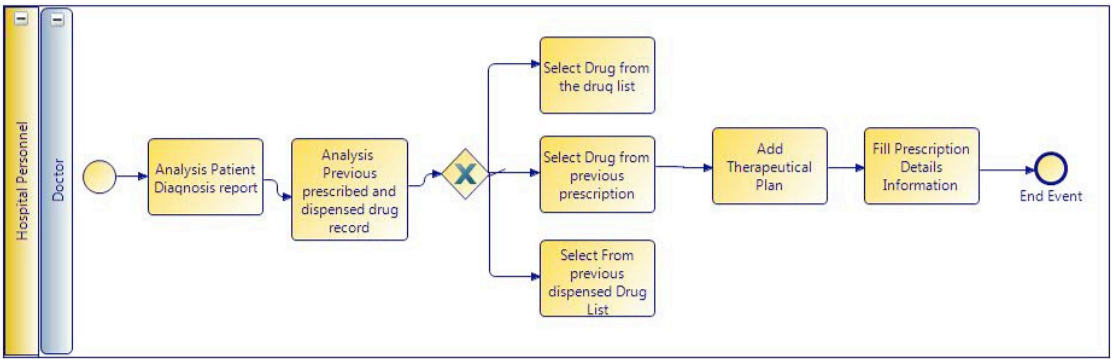

Figure 9.5: Generation of Prescription sub-process.

ment process as this incident does not follow healthcare regulation for drug reimbursement.

3. If the Prescriptions are not archieved correctly it affects the Drug reimbursement process as Drug Reimbursement report has to be produced from the prescription and dispensation data.

Chapter 10

Appendix B

Abstract

Generating report and sending it to the Healthcare Authority is the last phase of Drug Reimbursement process. The Accounting Office of the hospital generates the Drug Reimbursement reports for the Healthcare Authority from the Drug Prescription and Drug Dispensation information. The Administrative Officer of the Accounting Office retrieves and extracts the Drug Prescription and Drug Dispensation information of the hospital using the Hospital IT system and generates the Drug Reimbursement report following the Healthcare regulations. The reports are sent to the Healthcare Authority through the common e-mail systems using security mechanism that guarantees the confidentiality of the exchanged data.

10.1 Drug Reimbursement

In Italy, the outpatient drug reimbursement is regulated by the Ministry of Regional government. The Ministry dictates the regulations and guidelines for reporting reimbursable drugs to Regional Directorate through standard files and a standard process called Drug Reimbursement of File F. The Drug Reimbursement process is composed into four phases:

P1 : Drug Prescription

P2 : Drug Dispensation

P3 : Generation of File F report

P4 : Send File F report

Phase P1 and P2 are performed daily for each treatment to a patient, and P3 and P4 are performed monthly to prepare and send the File F report to the Healthcare Authority for the drug reimbursement. This case study emphasises on the reporting phase (P3 and P4), and describes in detail the business objectives, business processes, assets, actors and risks of this phase.

10.2 Business Objectives

- Generate the drug reimbursement report based on the prescription and dispensation information.
- Send the drug reimbursement report to the Healthcare Authority through an informative flow using security mechanism that guarantees the confidentiality of the exchanged data.

10.3 Assets

1. Document

   Drug Report contains the drugs information such as: name, type and price. It is generated by the Accounting office monthly for using in verification of drug reimbursement information. The pharmacy executes a sample check on the drug prices on the drug reimbursement data using the monthly Drug Report.

   Cost Center Report concerns about the drug information supplied at each Operational Unit. This report includes the name, type, quantity and the total drug price supplied to the Operational Unit. Accounting Office generates monthly the cost centre report and sends it to pharmacy. Using the Cost Centre report pharmacy checks that the drugs are correctly assigned to the O.U. and the declared quantity is reasonable.

   Drug Reimbursement Report is generated for the Healthcare Authority based on the prescription and dispensation information. It contains

drug name, total quantity, price of the drugs and personal identification of the patients.

2. Data

Prescription Data is the health-care program prescribed by the doctor to the patient. Prescription record includes:

- Patient Identity
- Diagnosis
- Doctor Identity
- Drug Name
- Drug type
- Drug Quantity
- Posology (Therapeutically Coverage)

Dispensation Data : Dispensation record includes the details information of the drug dispensed. Dispensation record includes:

- Patient Identity
- Dispensation Personnel
- Ref. to Prescription (If it exists)
- Drug Name
- Drug type
- Drug Quantity
- Drug Price

10.4 Actors

In Table 10.1, we illustrate actors and their responsibilities in the Report phase. Accounting Office, Hospital Pharmacy and Medical Direction Unit are part of the Hospital. HealthCare Authority supervises the hospital to observe healthcare regulation. Figure 10.1 shows the actor diagram of reporting phase.

Figure 10.2 shows the dependencies between the actors in reporting phase. Administrative Personnel of the Accounting office generates the monthly drug reimbursement report. Hospital is dependent on the accounting office for generating

Actor	Responsibility
Hospital	Provide Health-Care Service
Adm. Personnel	Process and Generate Drug Reimbursement Report
Accounting office	Generate Drug Report and Cost Centre Report
Hospital Pharmacy	Review and verify the Drug Reimbursement information through Drug and Cost centre Report. Validate the congruity of the archived prescription. Verify the prescription that is given to the hospitalized patient being prescribed as outpatient.
Medical Direction Unit	Send the Drug Reimbursement Report to the Healthcare Authority.
Healthcare Authority	Reimburse the drugs given to the patients. Surely, it also monitors the compliance of File F process execution towards the File F framework

Table 10.1: Actors' Responsibility in the Reporting Phase

and achieving the drug reimbursement report. The Administrative personnel of the Accounting office collect and extract the weekly drug reimbursement data from prescription and dispensation information. The Accounting office depends on the Pharmacy for the verification of the reimbursement data. Again for the verification of the reimbursement information Pharmacy needs the drug report and cost centre report. Pharmacy gets these reports from the Accounting Office. Medical Unit is responsible to send the drug reimbursement report to the HealthCare Authority and it relies on the Accounting Office for the drug reimbursement report.

10.5 Analysis of business processes

10.5.1 Business Process of Reporting phase

The administrative Officer of the Accounting Office generates the monthly drug reimbursement report following the Healthcare Regulation. The Accounting Office then sends the Drug Reimbursement report to the Medical Direction Unit who is responsible for sending the report to the Healthcare Authority. It sends the drug reimbursement report to the Healthcare Authority through an informative flow using security mechanism that guarantees the confidentiality of the exchanged

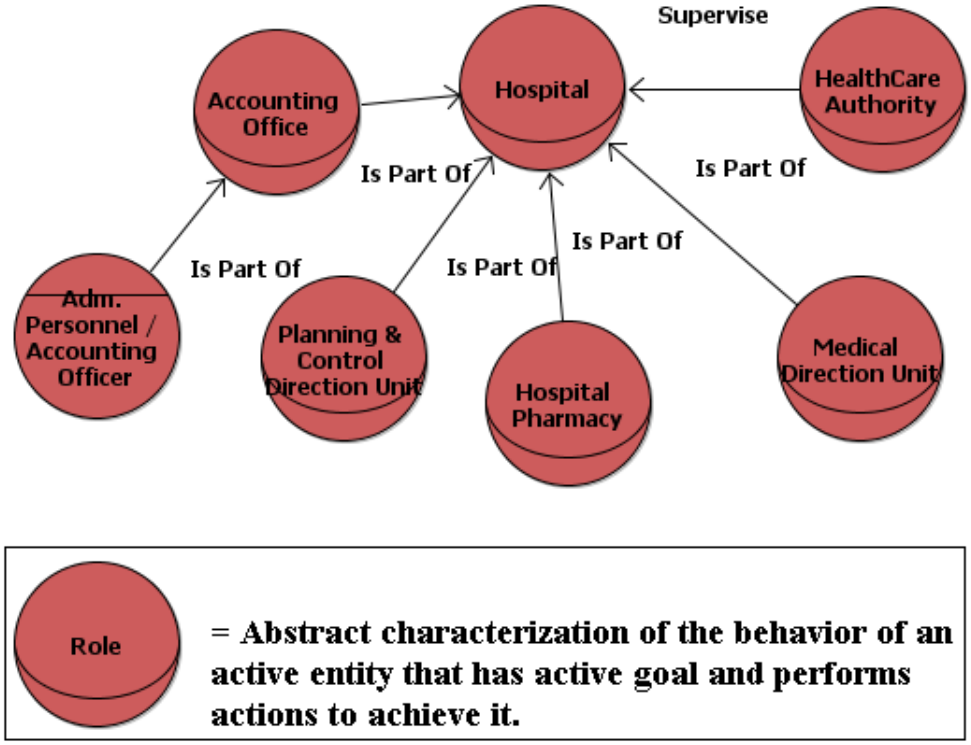

Figure 10.1: Actor diagram of the Report Generation and sending phase.

data. The overall business process of reporting phase is found in Figure 10.3.

For generating the monthly drug reimbursement report the administrative Officer of the Accounting Office needs to populate the drug reimbusement databse by weekly reimbusement data extraction. Business Process for weekly reimbursement data processing and the monthly Report generation is described in the following subsection.

10.5.2 Business Process of Data Processing and Report Generation

The administrative Officer of the Accounting Office extracts the drug reimbursement information weekly from the Drug Prescription and Drug Dispensation record and process the drug reimbursement information to populate the drug reimbursement database. This weekly data processing and verification procedure is shown

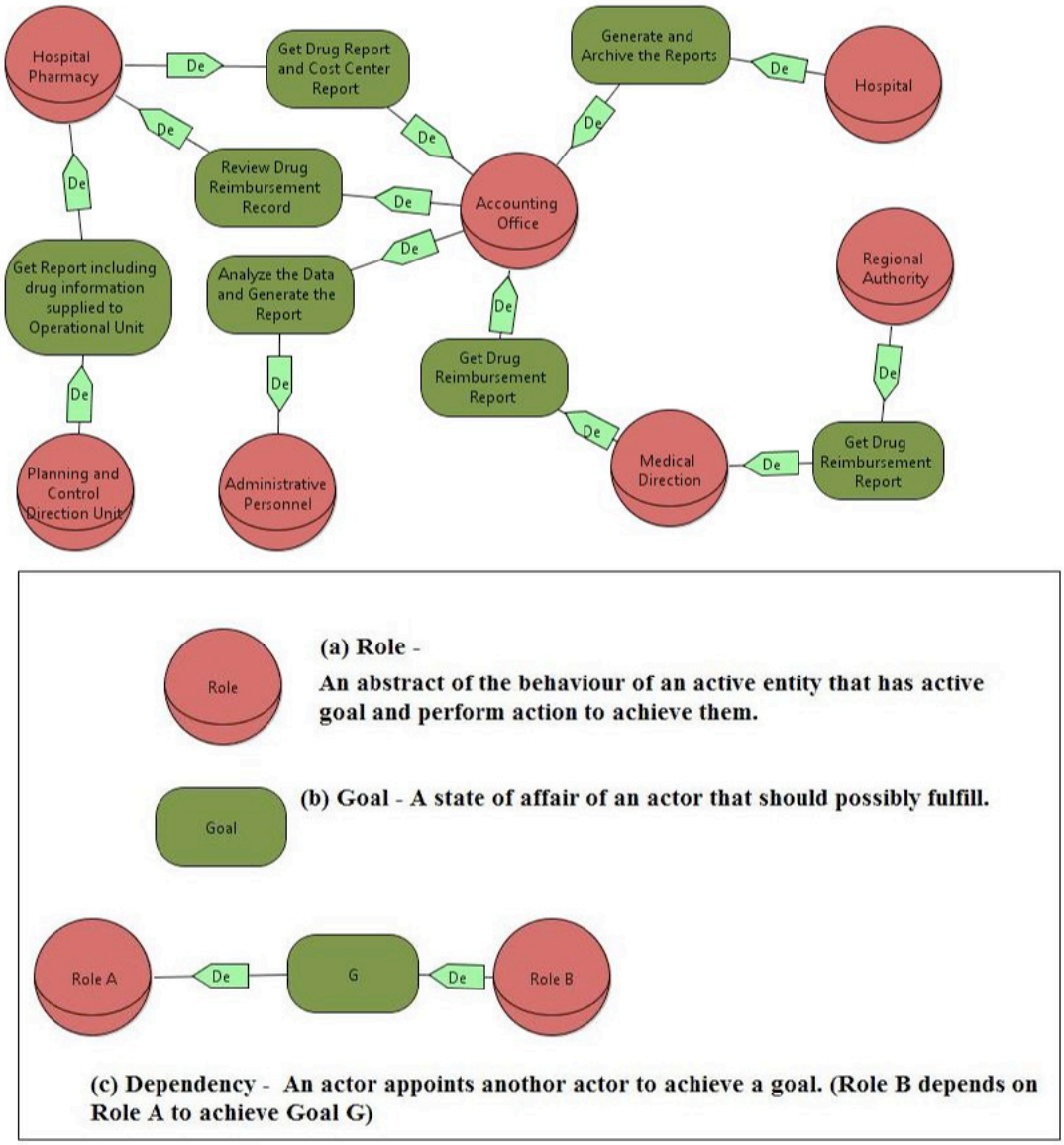

Figure 10.2: Reporting Phase

in figure 10.4.

Accounting office depends on the Pharmacy for the verification of the weekly drug reimbursement information. It sends the weekly archived prescription sheets to the pharmacy. The Pharmacy verifies the congruity of the prescription [1] and sends it back to Accounting Office, contacting also the reference doctor of the O.U. about errors in the prescription sheets. Then administrative Officer also

[1]Prescription and Dispensation information.

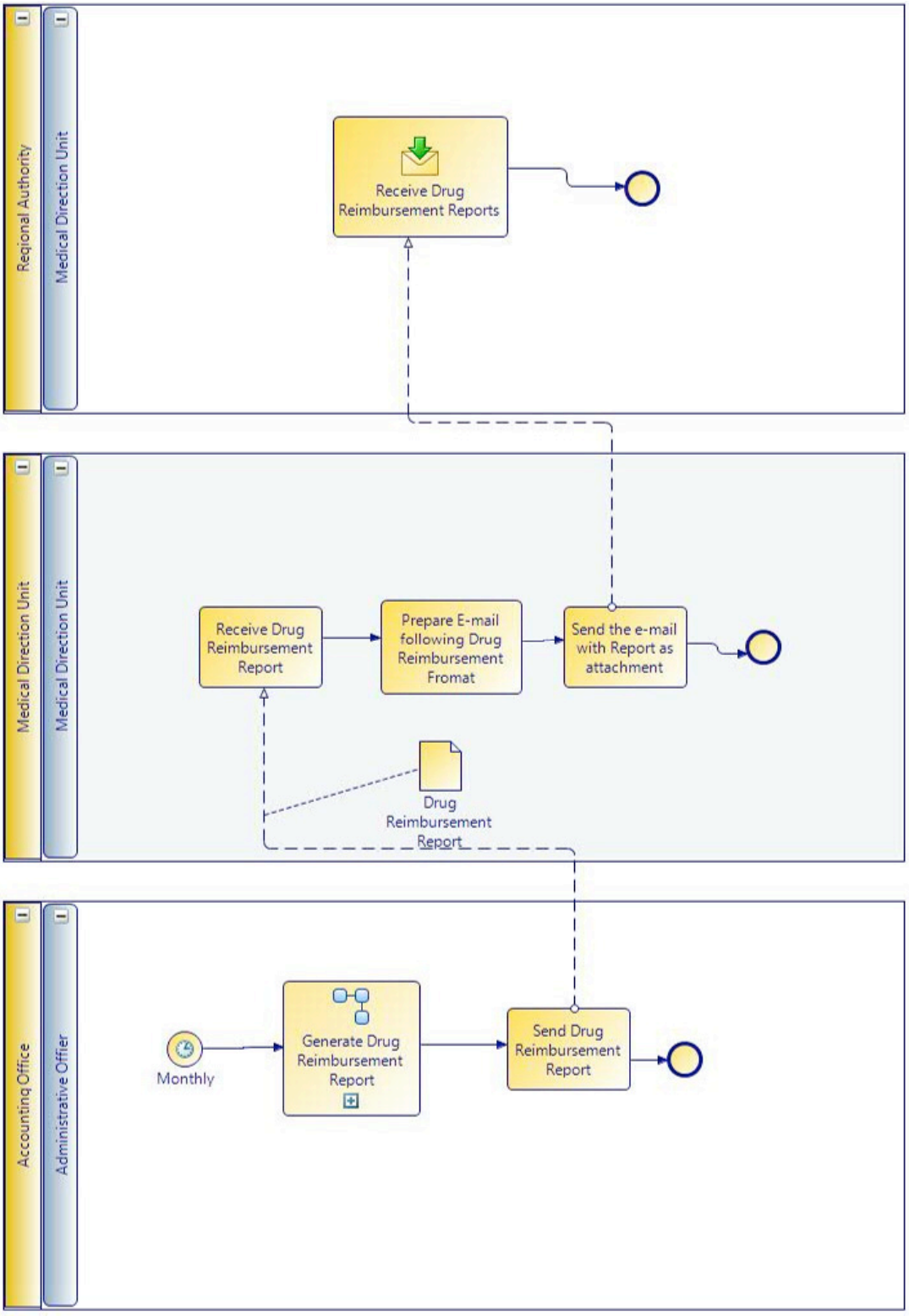

Figure 10.3: Business Process of the Reporting Phase.

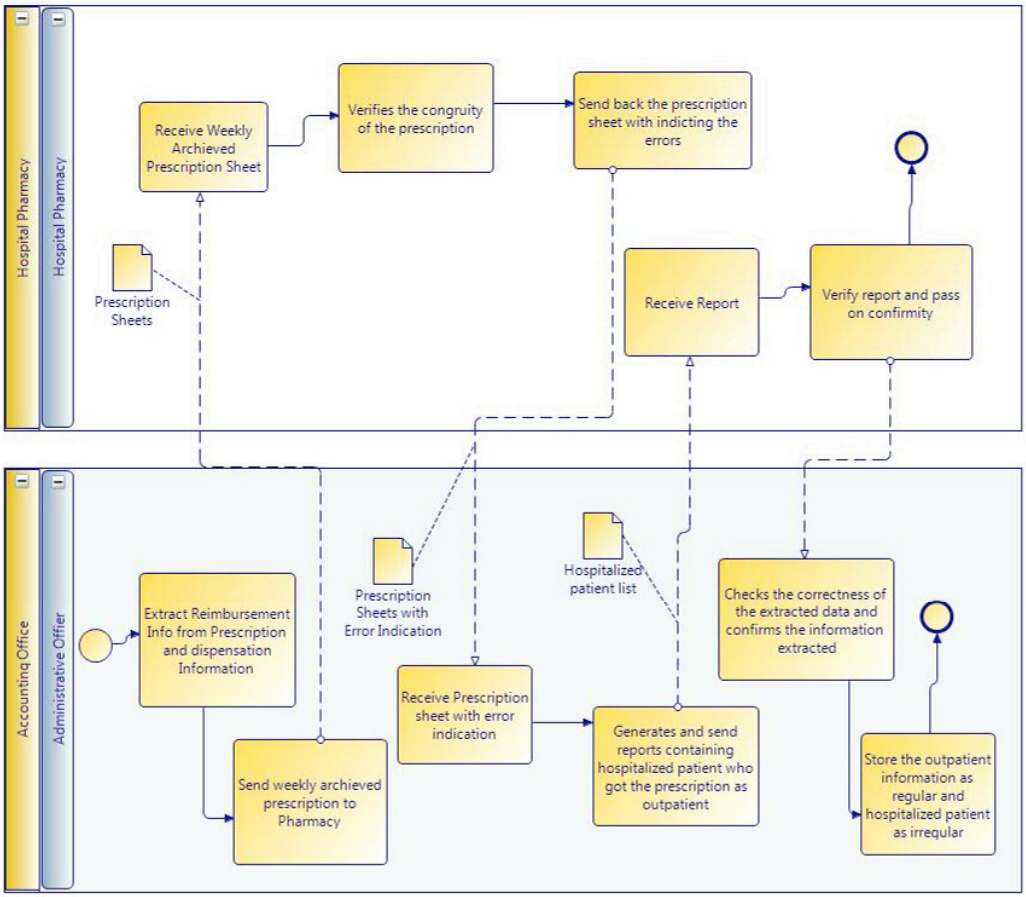

Figure 10.4: Business Process of weekly Drug Reimbursement Data Processing.

executes a control query in the system, generating a report containing the list of the patients who are hospitalized but being prescribed as outpatient. The Pharmacy performs a checking on the report containing the information of the hospitalized patient and send confirmation to the accounting office. Upon the confirmation the administrative officer entries the outpatient list as regular and hospitalized patient list as irregular data. Then this extracted data is used to consolidate the reimbursement database for generating monthly drug reimbursement report.

When the drug reimbursement database is populated for a month then Accounting office goes for generating the monthly drug reimbursement report. The monthly report generation process is shown in figure shown 10.5. Accounting Unit produces control prints such as Drug report and Cost Centre report and send those to the pharmacy monthly. The Pharmacy checks on the prices of the drug with

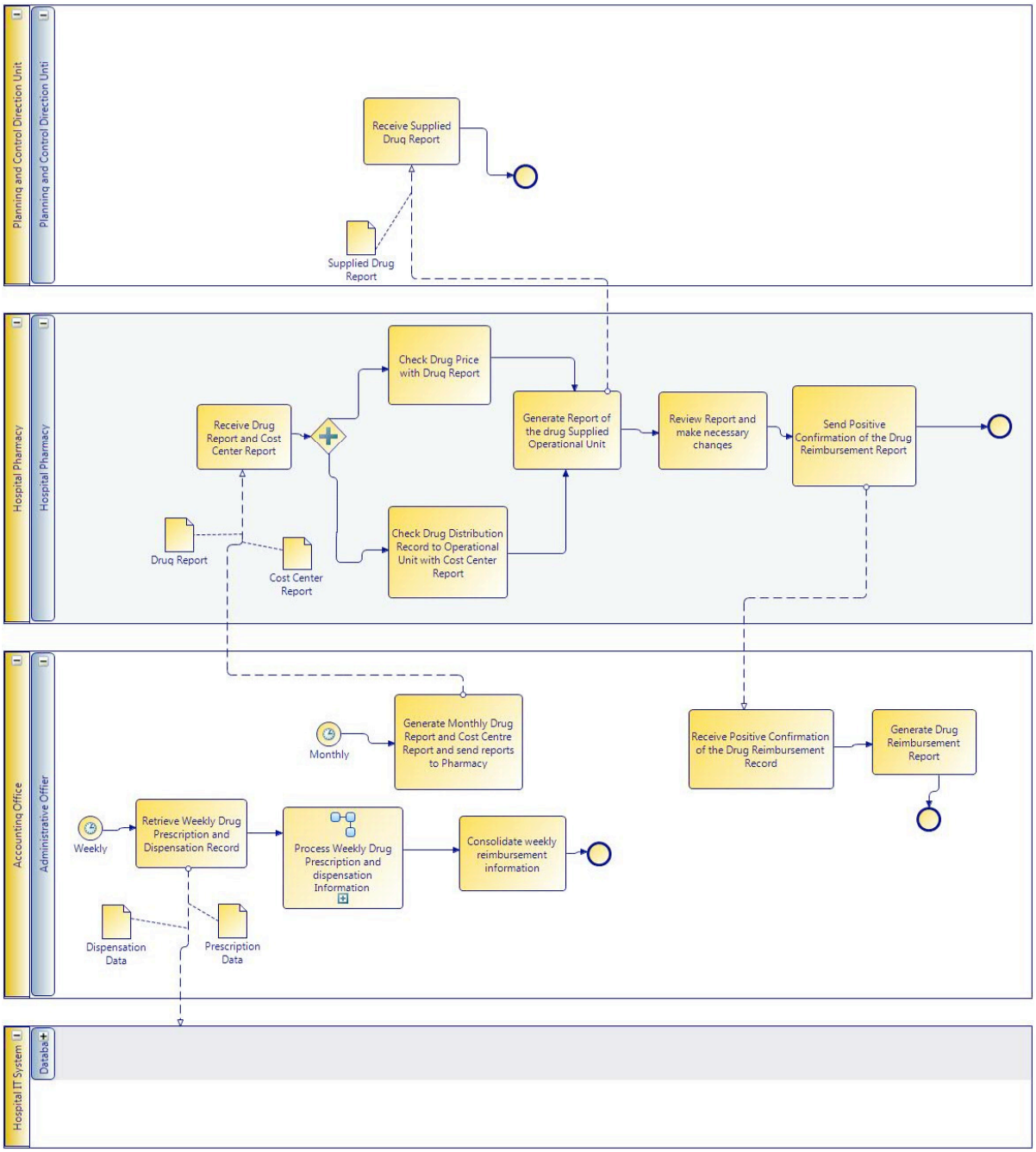

Figure 10.5: Business Process of Report Generation.

the drug report and with the Cost Centre report it checks that the drugs are correctly assigned to the O.U. and the declared quantity is reasonable. The Pharmacy generates a report with the quantity and the total value of the products delivered

to the Operational Unit and sends the report to Planning and Control Direction Unit for review. There the phase of control and execution is done upon the report with necessary changes and then the Pharmacy confirms to the Accounting Office that the drug reimbursement information is finalized following the Healthcare Regulation.

10.6 Regulatory Compliance

Regulatory Reference Italian Legislative Decree No. 196/2003 "Personal Data Protection Code": this law indicates the "Technical Specifications Concerning Minimum Security Measures" to apply to data processing done by electronic means. In particular in Annex B are specified the requirements about the "Computerized Authentication System", the "Authorization System", the "Security Policy Document", the "Additional Measures Applying to Processing of Sensitive or Judicial Data", etc. According to this regulation Hospital needs to protect personal, sensitive or judicial data against unauthorised access in sending to the HealthCare Authority through "debito informativo" channel.

Regulatory Reference Regional Circular No.5/SAN 30-1-2004 (and followings Circulars) indicate the guidelines for sending Drug Reimbursement report to Healthcare Authority. According to these regulations the Hospital has to produce the File F reports (FF1, FF2, FF3) including all the data required (personal data, data about drugs, etc.). moreover this regulation institutes the "debito informativo" channel to send the reports to the Authority (certified e-mail using cryptographic methods).

10.6.1 Reference indicating best practice

Reference "Governance, Leadership, and Direction" GLD.2 defined in Joint Commission Accreditation indicates the best practice where in Hospital a senior manager or director is responsible for operating the organization and complying with applicable laws and regulations.

Reference MCI.10 defined in Joint Commission Accreditation indicates the best practice for "Management of Communication and Information". Reference

MCI.10 indicates best practice for maintaining Information privacy and Confidentiality, reference MCI.11 indicates practice for maintaining Information security including data Integrity. MCI.18 reference defines protocol stating the requirements for developing and maintaining policies and procedures.

Reference "Patient and Relatives Rights " , "Standards and Measurable elements", PFR.1.2 and PFR.1.6 PFR.1.2 defined in Joint Commission Accreditation states the data protection and privacy of the personal information. According to this practice Hospital is respectful of the patient's need for privacy and also it treats the patient information as confidential information.

10.7 Risk of Report Generation and sending phase

1. Unauthorised access to the Reimbursement Database. This event violates the privacy consent of the patients by allowing access sensitive data to actors that are not related to the medical treatments.

2. Unauthorised modification to the drug reimbursement database. This risk makes the amount reimbursement incorrect (e.g., add false prescription and dispensation information or delete original reimbursement information) and surely it affects adversely either the hospital or the regional government.

3. Lack of making back-up of Drug Reimbursement records may hampers the drug reimbursement process if the original data is lost.

4. Delay in producing and sending the Drug Reimbursement Report to the Healthcare Authority results in the reimbursement delayed.

5. Sending the Drug Reimbursement Report through an insecure channel. It might compromise the confidentiality and integrity of the report.