

## Chapter 3

# A Guided Tour of the CORAS Method

This chapter presents a guided tour of the CORAS method. As illustrated by Fig. 3.1, the CORAS method is divided into eight steps. The first four of these steps are introductory in the sense that we use them to establish a common understanding of the target of the analysis, and to make the target description that will serve as a basis for the subsequent risk identification. The introductory steps include documenting all assumptions about the environment or setting in which the target is supposed to work, as well as making a complete list of constraints regarding which aspects of the target should receive special attention, which aspects can be ignored, and so forth. The remaining four steps are devoted to the actual detailed analysis. This includes identifying concrete risks and their risk level as well as identifying and assessing potential treatments for unacceptable risks.

In the following sections, we go through each of the eight steps of the CORAS method by means of a running example from the telemedicine domain. We follow two analysts in their interaction with an organisation by which they have been hired to carry out a risk analysis. They conduct the analysis according to the eight steps of the CORAS method.

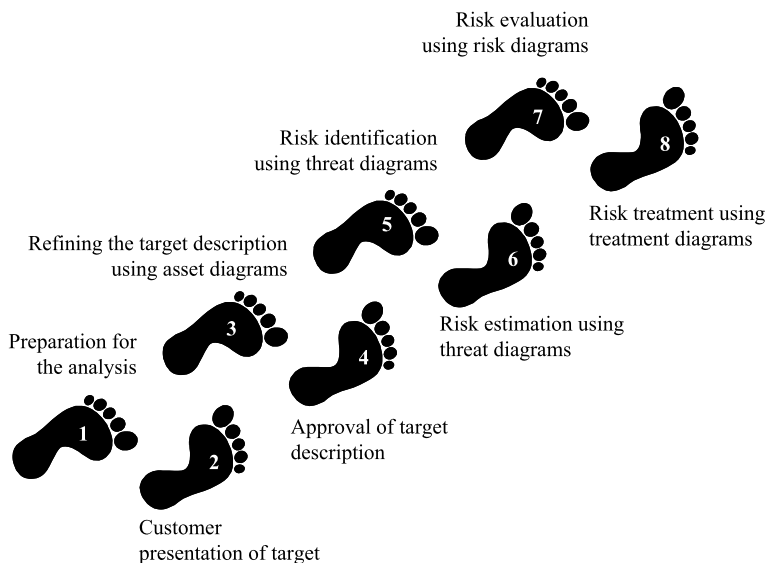
### 3.1 Preparations for the Analysis

The purpose of Step 1 is to do the necessary initial preparations prior to the actual startup of the risk analysis. This includes to roughly set the scope and focus of the analysis so that the analysis team can make the necessary preparations. It also includes informing the customer of its responsibilities regarding the analysis. We now introduce our example.

*Example 3.1* In one region of the country, an experimental telemedicine system has been set up. A dedicated network between the regional hospital and several primary

---

This chapter is an adaptation of the guided tour to the CORAS method presented in [10].



**Fig. 3.1** The eight steps of the CORAS method

health care centres (PHCC) allows a general practitioner (GP) to conduct a cardi-ological examination of a patient (at the PHCC) in cooperation with a cardiologist located at the hospital. During an examination, both of the medical doctors have access to the patient’s health record, and all data from the examination is streamed to the cardiologist’s computer.

The National Ministry of Health is concerned whether the patient privacy is suf-ficiently protected, and hires a risk analysis consultancy company to conduct a risk analysis of the cardiology system with particular focus on privacy. The consultancy company appoints a team of two consultants to do the job. They are in the following referred to as “the analysts” and assigned the roles of risk analysis leader and risk analysis secretary, respectively.

As a first step, the analysis leader organises a preparatory meeting with a rep-resentative from the ministry. At this meeting, the analysis leader is briefed and provided with documentation and background information. In particular, the rep-resentative from the ministry hands over the existing privacy regulations that the system should comply with. The analysis leader highlights the importance of hav-ing a fixed interaction point for the analysts at the ministry throughout the analysis. In particular, the ministry is asked to appoint one person that will serve as contact point and also be present at all important meetings throughout all of the subsequent steps of the analysis. The analysis leader also presents a plan for the analysis. It is decided that the effort on behalf of the analysts should be 200 man-hours and the plans are adjusted to fit with that. They also agree that the analysis should be completed within three months and a tentative meeting schedule is worked out. The analysis leader presents the objectives of the different meetings and what the objec-tives imply when it comes to selecting participants to the meetings. For example,

during risk identification it is important to involve technical expertise, while the presence of decision makers is essential at the initial meetings to help define the focus and scope of the analysis.

## 3.2 Customer Presentation of the Target

Step 2 involves an introductory meeting. The main item on the agenda for this meeting is to get the representatives of the customer to present their overall goals of the analysis and the target they wish to have analysed. Hence, during the second step, the analysts will gather information based on the customer's presentations and discussions.

Before starting to identify and analyse potential risks to something, it is necessary to know exactly what this something is. What is the scope of the analysis, and what are the assumptions that we may make? In other words, we need to know what we are supposed to protect before we can start finding the threats against it and how it may be harmed, as well as how it should be protected. It is furthermore essential that the parties of the risk analysis and the analysts agree on a common terminology and how it should be used. They also need to arrive at a joint understanding of what should be the target of analysis, the assets to protect, the scope and focus, as well as all assumptions being made.

*Example 3.2* A meeting is organised where, in addition to the analysts and a representative from the ministry, the IT manager of the regional hospital and a general practitioner from one of the PHCCs participate.

This meeting is where the overall setting of the analysis is decided, and the first step is taken towards establishing the target description that will be used later in the analysis. The meeting starts with the risk analysis leader giving a brief presentation of the method to be used, what the customer (the National Ministry of Health) can expect from the analysis, and a proposed meeting schedule. The analysis leader reminds the representative of the ministry of the responsibilities with respect to providing necessary information and documentation about the target in question, as well as allocating people with suitable background to participate at the scheduled meetings and workshops.

The IT manager then presents the telemedicine system intended as target. As part of the presentation, she draws the picture shown in Fig. 3.2. From the picture, we see that speech and other data from the examination of a patient is streamed over a dedicated network, while access to the patients' health record (stored in a database at the regional hospital) is given through an encrypted channel over the Internet. Next in line after the IT manager is the medical doctor from the PHCC. She talks about her personal experiences from using the system.

After the presentations, a discussion on the scope and focus of the analysis follows. The representative of the ministry emphasises that they are particularly worried about the confidentiality and integrity of the health records and other medical data, first and foremost for the sake of the patients' health, but also because of the

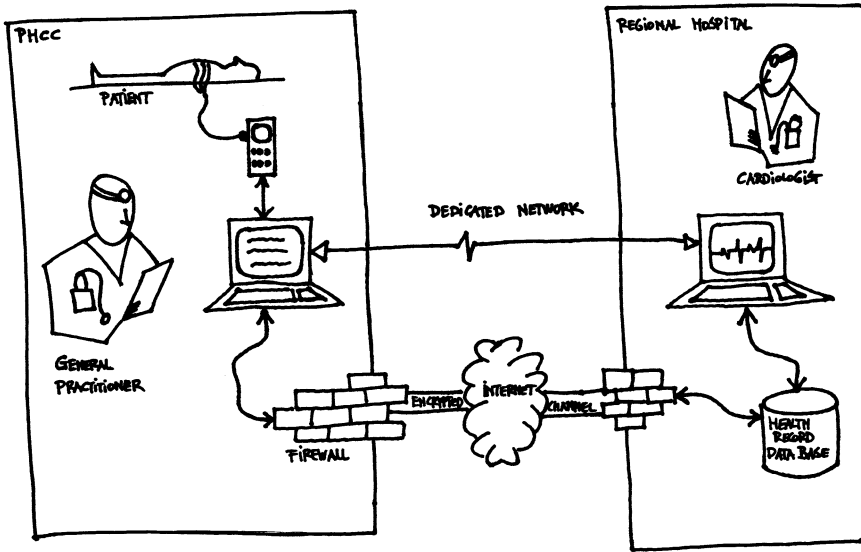


Fig. 3.2 Picture of target

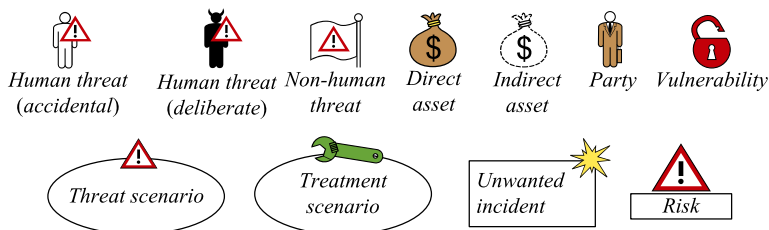
public's trust in the national health care system. For the medical doctor, the most important thing is the patients' health and well-being, and hence also the availability and integrity of the telemedicine system. The IT manager explains that they have already made a security analysis of the health record database and the encrypted access, so she is confident that this part of the system is secure and reliable. After some discussion, the representative of the ministry decides that the focus will be on confidentiality and integrity of medical data, and the availability of the service, but that the access to the health record database is outside the scope of analysis.

As the last point on the agenda, the participants set up a plan for the rest of the analysis with dates for meetings and delivering of reports, as well as indications of who should attend the various meetings.

### 3.3 Refining the Target Description Using Asset Diagrams

The objective of Step 3 is to arrive at a more correct and refined understanding of the target and the objectives of the customer. Also this step typically involves a meeting between the analysts and the representatives of the customer. The meeting is divided into three parts: (1) presentation of the target as understood by the analysts; (2) asset identification; (3) high-level risk analysis.

The purpose of the presentation of the of the target by the analysts is to correct misunderstandings on behalf of the analysts and to settle issues in need of clarification. The asset identification involves pinpointing the most important valuables of the parties of the analysis. The parties typically include the customer, but may also



**Fig. 3.3** Symbols of the CORAS risk modelling language

be other relevant stakeholders with respect to the target in question. The assets are the things or entities that these parties want to protect, and are the real motivation for conducting the risk analysis in the first place. The identified assets are documented using so-called asset diagrams. Asset diagrams are one of five kinds of diagrams offered by the CORAS risk modelling language. The other four play important roles in later steps of the CORAS method as we will see. Common for all five kinds of diagrams is that they make use of partly overlapping subsets of the graphical symbols presented in Fig. 3.3. In the case of asset diagrams, the subset consists of the two symbols for asset, and the one for party.

The main purpose of the high-level analysis is to get an overview of the main threats and risks with respect to the identified assets, in particular, at an enterprise level and from the perspective of the decision makers. The high-level analysis helps the analysts in identifying the aspects of the target that have the most urgent need for in-depth analysis, and hence makes it easier to define the exact scope and focus of the full analysis.

*Example 3.3* The meeting starts with the analysis leader presenting the analysts' understanding of the target to be analysed. The analysts have formalised the information presented by the customer at the previous meeting, as well as the documentation received in the mean time. It was decided to use UML for this formalisation. The UML class diagram of Fig. 3.4 shows the relevant concepts and how they relate to each other, while the UML collaboration diagram of Fig. 3.5 illustrates the physical organisation of the target. Furthermore, the medical doctor's description of use has been captured as a UML activity diagram as shown in Fig. 3.6. During this presentation, the participants representing the customer make corrections and eliminate errors, so that the result is a target description that all parties can agree upon. In the class diagram and the collaboration diagram, the analysis leader has also indicated what he understands is the scope of the analysis.

After agreeing on a target description, the analysis moves on to asset identification. An asset is something in or related to the target to which the customer or other party of the analysis assigns great value. Based on the discussion at the introductory meeting, the analysis leader has prepared the initial *CORAS asset diagram* of Fig. 3.7 to help specifying the scope of the analysis. The asset diagram shows the National Ministry of Health as the party on whose behalf the assets are identified, and its four assets *Health records*, *Provision of telecardiology service*, *Patients'*

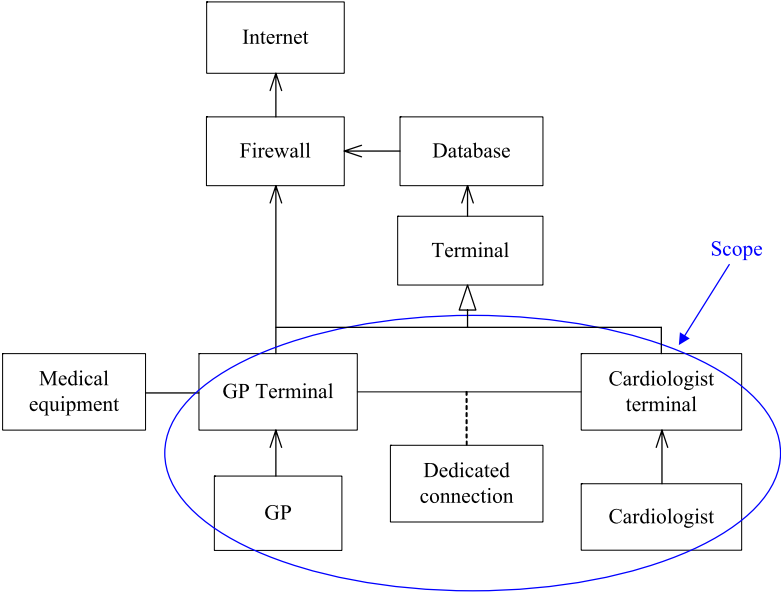


Fig. 3.4 Class diagram showing the target concepts

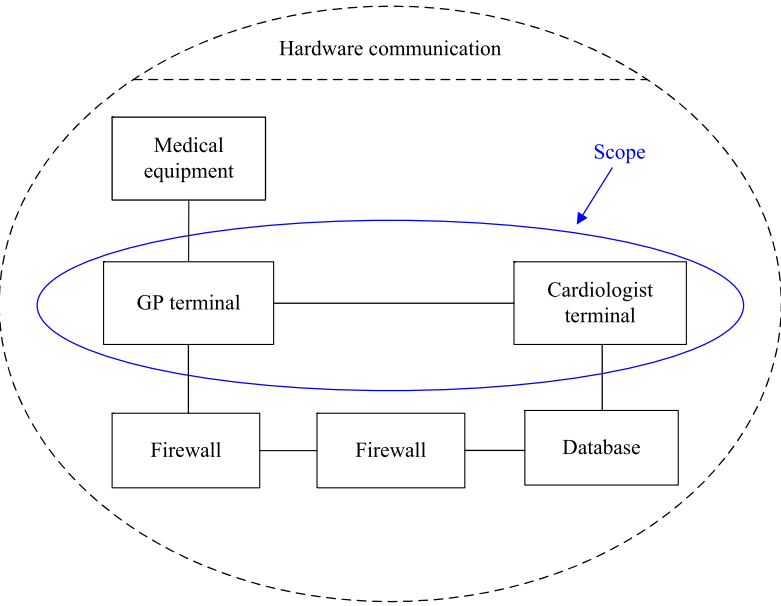
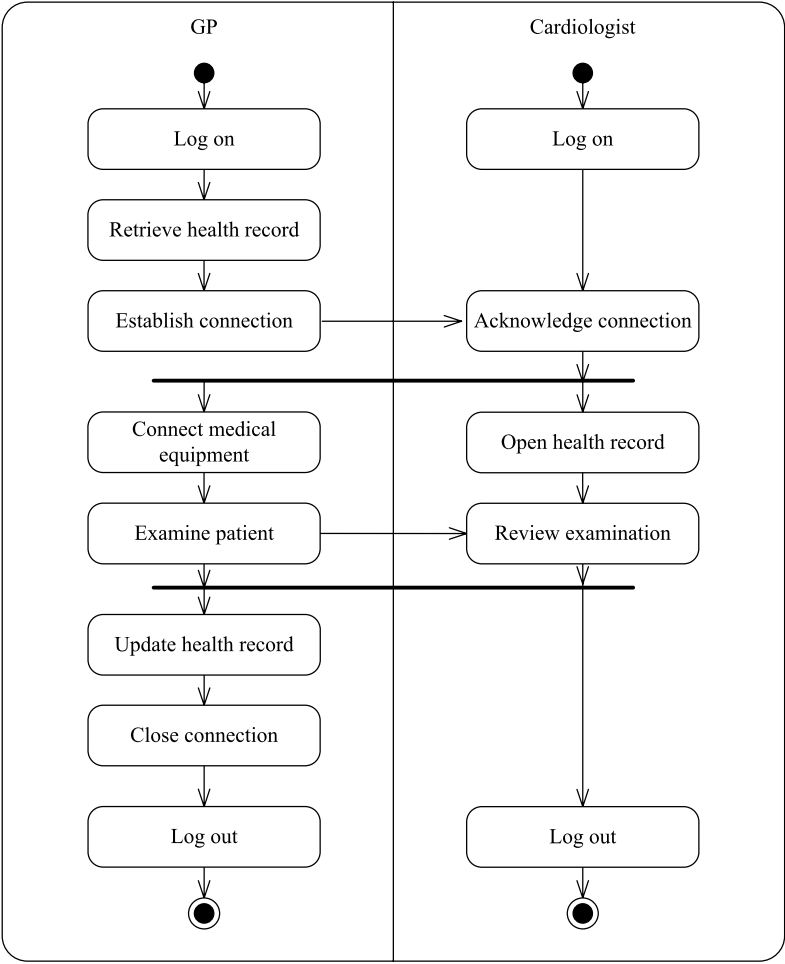


Fig. 3.5 Collaboration diagram illustrating the physical communication lines



**Fig. 3.6** Activity diagram describing the parallel processes of the GP and the cardiologist

*health* and *Public’s trust in system*. The arrows show dependencies between the assets, such that for example, harm to *Health records* may cause harm to *Public’s trust in health care system*.

The analysis leader explains that *Public’s trust in system* is represented with a slightly different symbol than the other three because this is a so-called indirect asset. He goes on to explain that an asset is indirect if, with respect to the target of analysis, it is harmed only through harm to other assets. The remaining assets are direct. In Steps 4, 5 and 6, the indirect asset may to a large extent be ignored since risks with respect to this asset can be identified by identifying risks with respect to the direct assets. The analysts still need to provide a risk picture for the indirect asset during the risk evaluation of Step 7. It follows from the diagram that risks to

Fig. 3.7 Asset diagram

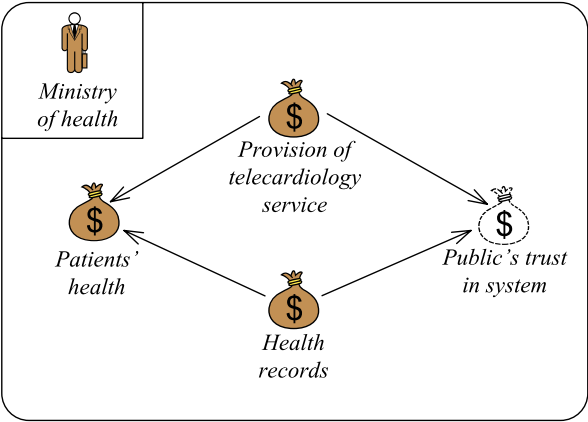


Table 3.1 High-level risk table

Who/what causes it?	How? What is the incident? What does it harm?	What makes it possible?
Hacker	System break-in and theft of health records	Insufficient security
Employee	Sloppiness compromising confidentiality of health records	Insufficient training
Eavesdropper	Eavesdropping on dedicated connection	Insufficient protection of connection
System failure	Service failure during examination	Unstable connection/immature technology
Employee	Sloppiness compromising integrity of health records	Prose-based health records (i.e., natural language)
Network failure	Transmission problems compromising integrity of medical data	Unstable connection/immature technology
Employee	Health records leak by accident, compromising confidentiality and damaging the trust in the system	Possibility of irregular handling of health records

*Public's trust in system* are identified via risks to *Health records* and *Provision of telecardiology service*. The asset *Patients' health* may also be harmed via harm to the latter two, but may also be harmed directly in other ways within the scope of the analysis and is therefore specified as a direct asset.

After agreeing on the assets, the analysts conduct a high-level analysis. The short brainstorming should identify the most important threats and vulnerabilities with respect to the identified assets, without going into great detail. In this case, the cus-

customer is concerned about hackers, eavesdroppers, system failure and whether the security mechanisms are sufficient. These threats and vulnerabilities do not necessarily involve major risks, but give the analysis leader valuable input on where to start the analysis. The analysis secretary documents the results by filling in the high-level risk table shown in Table 3.1. The symbols above the three columns indicate what kind of information should be documented.

### 3.4 Approval of the Target Description

Step 4 also typically involves a separate meeting, but may alternatively be conducted by email or other means of communication. The main objective of Step 4 is to agree on the description of the target to be analysed, including scope, focus and all assumptions, and for the customer to approve the description. Important aspects of the target documentation are definitions of scales for likelihoods and consequences as well as risk evaluation criteria. The formulation of these aspects are subtasks of Step 4.

We often need multiple consequence scales, which are used when it is difficult or inappropriate to measure or describe damage to all assets according to the same scale. It is easier, for example, to measure income in monetary values than to do the same for company brand. There should only be one likelihood scale for the analysis based, for example, on time-intervals such as years, weeks and hours, or on probabilities. The last activity of the approval step is to decide upon the risk evaluation criteria. These criteria characterise the minimal level of risk required for risks to deserve a detailed evaluation for possible treatment. Step 4 should not terminate before the full documentation as prepared by the analysts has been approved by the customer.

*Example 3.4* The analysis leader has updated his presentation from the last meeting based on input and comments that he received from the representatives of the customer during Step 3, and the target and asset descriptions are now to be finally approved. Based on the discussions at the previous meetings and the issues identified in the high-level analysis, the customer and the analysis team decided to narrow the scope of the analysis, and agree upon the following target definition:

The target of analysis is the availability of the telecardiology service, and confidentiality and integrity of health records and medical data in relation to use of the service and related equipment.

An unwanted incident is an event that when it occurs harms or reduces the value of at least one of the identified assets. A risk is a characterisation of the severity of an unwanted incident with respect to a single asset. If an unwanted incident harms more than one asset, we get a separate risk for each of the harmed assets. Typically the customer is forced to accept some risks, either because of shortage of resources, conflicting concerns or because the treatment costs will be greater than the benefits. As a first step towards distinguishing risks that can be accepted from those that

**Table 3.2** Asset table

Asset	Importance	Type
Health records	2	Direct asset
Provision of telecardiology service	3	Direct asset
Public's trust in system	2	Indirect asset
Patients' health	1	Direct asset

**Table 3.3** Likelihood scale

Likelihood value	Description	Definition
Certain	Five times or more per year	$[50, \infty) : 10y = [5, \infty) : 1y$
Likely	Two to five times per year	$[20, 50) : 10y = [2, 5) : 1y$
Possible	Less than twice per year	$[5, 20) : 10y = [0.5, 2) : 1y$
Unlikely	Less than once per two years	$[1, 5) : 10y = [0.1, 0.5) : 1y$
Rare	Less than once per ten years	$[0, 1) : 10y = [0, 0.1) : 1y$

cannot, the representatives of the customer are asked to rank the assets according to their importance (1 = very important, 5 = minor importance) and fill in the asset table as shown in Table 3.2.

Having finished the asset table, they go on to define the likelihood scale and the consequence scales. A likelihood is a general description of the frequency or probability for incidents to occur, and the likelihood scale defines the values that will be used when assigning likelihood estimates to unwanted incidents. A consequence is a description of the impact of unwanted incidents on the assets in terms of degree of damage, and the consequence scale defines the values that will be used when estimating the impact of unwanted incidents.

The analysts initiate the discussion by suggesting a scale of likelihood based on the following rule of thumb: The lowest likelihood *rare* is set to be maximum one occurrence during the target's lifetime; the remaining intervals have an increasing number of expected events until the maximum possible number of incidents per year is reached. Table 3.3 gives the likelihood scale defined for the target of analysis. The likelihood *possible*, for example, denotes less than twice a year, which is defined by the precise interval from 5 to 20 occurrences per 10 years, as shown in the table. By using the same scale for all scenarios and incidents, it is possible to extract combined likelihood values as shown later in the risk estimation step.

Because incidents may have different impact depending on which asset is harmed, they decide to make a separate consequence scale for each of the direct assets. Table 3.4 shows the consequence scale defined for the asset *Health records* in terms of number of health records that are affected. If desired, the consequence description for an asset may include more than one measure. For example, *major* could be the number of disclosed health records, the number of deleted records, and so forth.

**Table 3.4** Consequence scale for *Health records*

Consequence value	Description
Catastrophic	1000+ health records are affected
Major	101–1000 health records are affected
Moderate	11–100 health records are affected
Minor	1–10 health records are affected
Insignificant	No health records are affected

**Table 3.5** Risk evaluation matrix

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare					
	Unlikely					
	Possible					
	Likely					
	Certain					

Finally, the representatives of the customer define the risk evaluation criteria. The risk evaluation criteria assert whether a risk to an asset should be evaluated further or not. A risk that is not accepted according to the risk evaluation criteria may nevertheless have to be accepted as a result of the cost-benefit analysis conducted when deciding how to respond to the conclusions from the risk analysis. They define these criteria by means of a risk evaluation matrix for each asset. The risk analysis leader draws the matrix for the asset *Health records* on a blackboard. It has likelihood and consequence values as its axes so that a risk with a specific likelihood and consequence will belong to the intersecting cell. Based on a discussion in the group, the risk analysis leader marks the cells in the matrix as either *acceptable* or *unacceptable* (i.e., *must be evaluated*) by filling the cells with the colour green or red, respectively. The resulting risk evaluation matrix is shown in Table 3.5. The participants decide to use these criteria for the other assets as well.

After all this has been approved by the customer, including the target description with the target models, the analysts have the framework and vocabulary they need to start identifying threats (a potential cause of an unwanted incident), vulnerabilities (weaknesses which can be exploited by one or more threats), unwanted incidents and risks.

3.5 Risk Identification Using Threat Diagrams

Step 5 is organised as a workshop gathering people with expertise on the target of analysis. The goal is to identify as many potential unwanted incidents as possible, as well as threats, vulnerabilities and threat scenarios.

To do this identification, we make use of a technique called structured brainstorming. Structured brainstorming may be understood as a structured walk-through

of the target of analysis and is carried out as a workshop. The main idea of structured brainstorming is that since the participants of the analysis represent different competences, backgrounds and interests, they will view the target from different perspectives and consequently identify more, and possibly other, risks than individuals or a more homogeneous group would have managed.

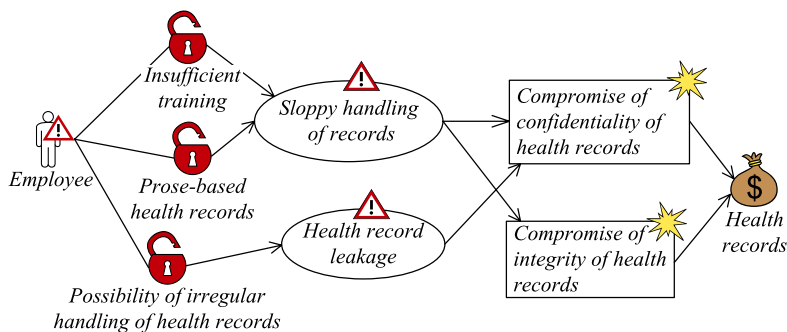
The findings of the brainstorming are documented using CORAS threat diagrams, which are the second kind of diagrams offered by the CORAS risk modelling language.

*Example 3.5* The analysis leader challenges the participants to work with questions like: What are your biggest concerns with respect to your assets? (Threat scenarios and unwanted incidents.) Who/what may initiate threat scenarios and unwanted incidents? (Threats.) What makes this possible? (Vulnerabilities.) The answers are documented by the secretary on-the-fly using CORAS threat diagrams that are displayed to the participants.

The analysis leader has used this technique on numerous occasions before. He does not employ exactly the same procedure in every case, but adapts it to fit the target domain. He often finds it useful to include checklists and “best practices” for a specific technology or domain. In this case he needs IT experts and medical personnel (general practitioners) to participate in the brainstorming, but some will only participate when their competences are needed for specific scenarios. Since people may be involved at different stages of the analysis, it is essential that information gathered during this session is documented in a simple and comprehensive way.

The analysis leader uses the target models approved during Step 4 as input to the brainstorming session. The models, as exemplified by Figs. 3.4, 3.5 and 3.6, are assessed in a stepwise and structured manner and the identified unwanted incidents are documented on-the-fly.

A set of initial, preliminary threat diagrams has been prepared by the analysis team on the basis of the high-level analysis table shown in Table 3.1. Three of these threat diagrams are shown in Figs. 3.8, 3.9 and 3.10. These may represent a starting point for discussion. The analysis team has structured the three diagrams according to the different kinds of threats: human accidental, human deliberate and



**Fig. 3.8** Initial threat diagram for accidental actions

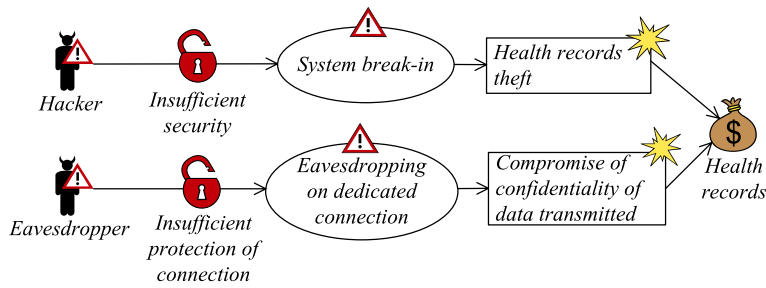


Fig. 3.9 Initial threat diagram for deliberate actions

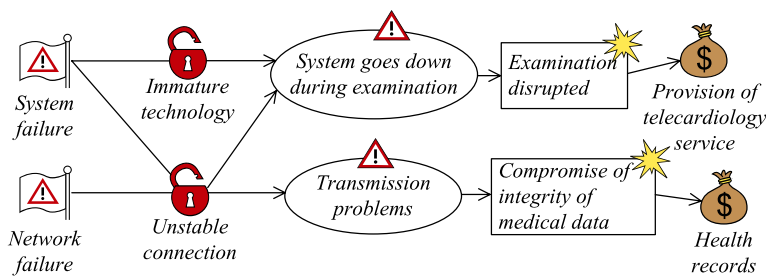


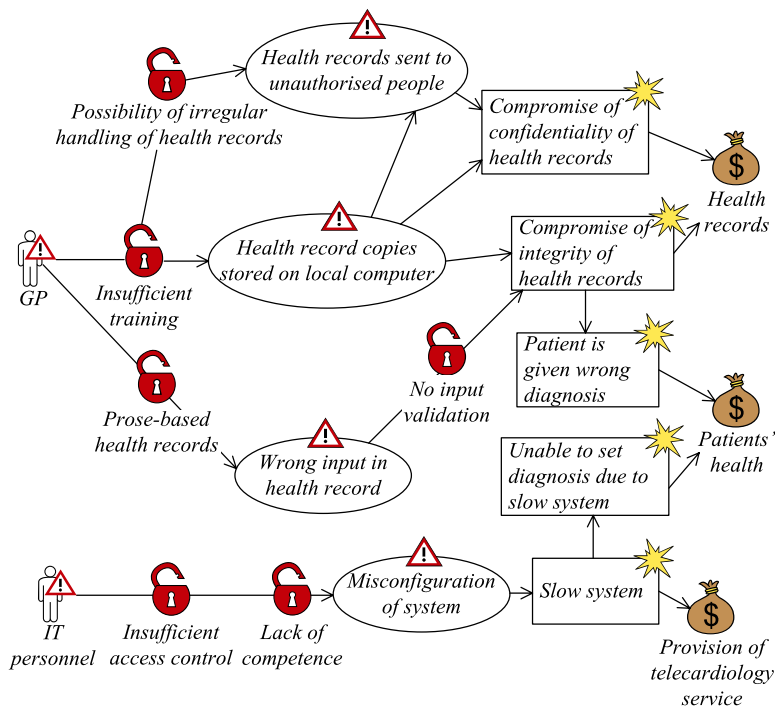
Fig. 3.10 Initial threat diagram for non-human threats

non-human threats. To what extent these diagrams are presented to the participants of the brainstorming session is dependent on the situation. In any case, these initial threat diagrams provide helpful guidance to the analysis leader with respect to what aspects on which to focus.

The threat diagram in Fig. 3.8 shows how a combination of insufficient training or prose-based health records together with sloppiness may compromise the integrity and confidentiality of the patients' health records. The system also allows for irregular handling of health records with the result that an employee accidentally may cause a leakage of records. A confidentiality or integrity breach may harm the health record in the sense that it no longer is secret or correct, respectively. In the extreme consequence, a faulty health record may affect the patients' health.

In the threat diagram of Fig. 3.9 that describes deliberate harmful actions caused by humans, the participants have identified two main threats, namely hacker and eavesdropper. A hacker may exploit insufficient security mechanisms to break into the system and steal health records. An eavesdropper is someone who, due to insufficient protection of communication lines, may gather data that is transmitted and thereby compromise its confidentiality.

The participants also worry about threats like system failure and network failure, as documented in Fig. 3.10. They fear that unstable connections or immature technology are vulnerabilities that may lead to system crashes during examination or transmission problems. A transmission problem may interfere with the data that is stored in the system and leave the health records only partly correct.



**Fig. 3.11** Final threat diagram for accidental actions

During the brainstorming session, the initial threat diagrams are expanded with new information on-the-fly. The diagrams may require updating and polishing after the session has ended. The threat diagram of Fig. 3.8 illustrating incidents caused by accidental actions of employees receives much attention among the participants and develops into the diagram shown in Fig. 3.11. In the following, we concentrate on just this one, and do not explore the other two threat diagrams further.

The participants decide that the threat *Employee* must be split into *general practitioner (GP)* and *IT personnel* since they may cause different incidents. If the GP has too little security training, she may store copies of health records on a local computer. This may compromise the integrity of the records and in the worst case lead to an erroneous diagnosis of a patient. The same incidents may also occur if the GP enters wrong information into the patients' health record. The system allows for irregular handling of health records which opens for the possibility of accidentally sending records to unauthorised people. This would compromise the confidentiality of the health record. The policy of the IT personnel with respect to access control has been very "loose". They explain this with their responsibility for making critical updates in emergencies and that they do not have the time to wait for personnel with correct access rights to show up. An unfortunate consequence of this is that personnel without the required competence sometimes become responsible for critical changes. This may lead to misconfiguration of the system, which again may

slow the system down. If the system is too slow it may be impossible to set a patient's diagnosis, and also the ability of providing a telecardiology service may be compromised.

### 3.6 Risk Estimation Using Threat Diagrams

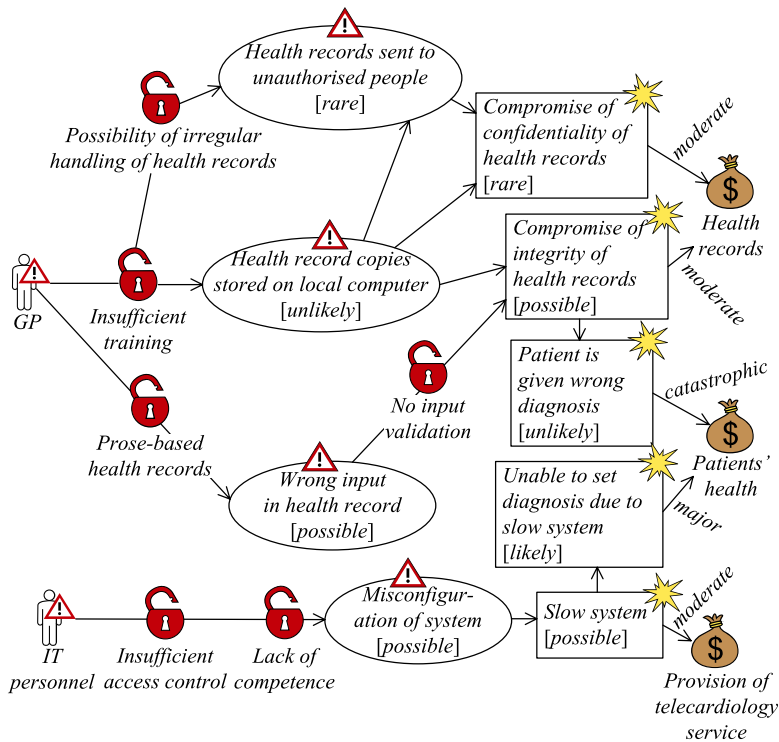
When the threat scenarios, unwanted incidents, threats and vulnerabilities are properly described in threat diagrams it is time to estimate likelihoods and consequences. This is the main task of Step 6 which is also typically conducted as a structured brainstorming. The likelihoods and consequences are needed in order to compute the risk values which are used to decide whether risks are acceptable or should be further evaluated for possible treatment.

The participants of the brainstorming session provide likelihood estimates based on their judgements or give advice with respect to how they may be determined from historical data that they are aware of. Since risk values are calculated from the likelihoods of unwanted incidents, and not threat scenarios, the unwanted incidents are the main focus of the likelihood estimation. However, if the likelihood of an unwanted incident is hard to determine or very uncertain, we may try to deduce the value from the likelihoods of the threat scenarios and unwanted incidents to which they are directly related. The documentation of information about the likelihoods of threat scenarios is useful also because it shows the most important sources of risks. This gives a more detailed risk picture and furthermore serves as a basis for determining where to direct treatments.

Consequences are estimated for each relation from an unwanted incident to an asset. The consequence values and the likelihood values are taken from the consequence scale of the asset and the likelihood scale, respectively, as defined during Step 4.

*Example 3.6* The analysis leader organises the risk estimation as a separate workshop with a structured brainstorming where the starting point is the threat diagrams from the previous workshop. He knows that in this workshop it is especially important to include people with diverging backgrounds and competences, such as users, technical experts and decision makers. The participants of the analysis decide that “most likely” estimates will provide more realistic risk values than “worst case” estimates. First, they provide as many estimates as possible for the threat scenarios, which in turn facilitates the estimation of the likelihood of the unwanted incidents. Second, the consequences of the unwanted incidents for each harmed asset are estimated. The estimates are documented by annotating the diagrams as shown in Fig. 3.12.

There are different ways of computing the likelihood of an incident that may be caused by more than one threat scenario. If the estimates are suitable for mathematical calculations a computerised tool may be used. Since the likelihood scale in our case is in the form of intervals, the analysis leader decides to use an informal method that is quite straightforward and transparent. The threat scenario *Health records sent*



**Fig. 3.12** Threat diagram with likelihood and consequence estimates

**Table 3.6** Combined likelihood estimates

Threat scenario	Likelihood	Unwanted incident	Combined likelihood
Health records sent to unauthorised people	Rare ([0, 1) : 10y)	Compromise of confidentiality of health records	[0, 1) : 10y + [1, 5) : 10y = [1, 6) : 10y
Health record copies stored on local computer	Unlikely ([1, 5) : 10y)		It is decided that <i>unlikely</i> is the best fit

to unauthorised people and Health record copies stored on local computer can both lead to Compromise of confidentiality of health records. Table 3.6 shows the rough estimation of the combined likelihood. The technique is informal, but suitable for the creative setting of a structured brainstorming. It is of course important that the combined estimates reflect reality, meaning that the combined estimates should be presented to the participants for validation or adjustment.

As shown by Table 3.6, the aggregated likelihood of the two threat scenarios is [1, 6) : 10y which is overlapping both *unlikely* and *possible*. Since the aggregated

interval hardly intersects with *possible*, and since it clearly gravitates towards *unlikely*, the latter is chosen to represent the aggregation.

However, although the aggregation of the likelihoods of the two threat scenarios yields *unlikely*, it may still not be that this value correctly represents the likelihood of the unwanted incident *Compromise of confidentiality of health records*. This is because the storage of health records on a local computer not necessarily leads to the compromise of the records. In fact, the participants in the brainstorming group reject the suggested estimate for *Compromise of confidentiality of health records*, arguing that the likelihood is less than *unlikely*. The value is therefore adjusted to *rare*, as documented in the threat diagram of Fig. 3.12.

### 3.7 Risk Evaluation Using Risk Diagrams

Step 7 involves giving the customer the first overall risk picture. This will typically trigger some adjustments and corrections of the information documented so far. The objective of the risk evaluation is to determine which of the identified risks that must be considered for possible treatment based on the risk estimation of the previous step, as well as the risk evaluation criteria.

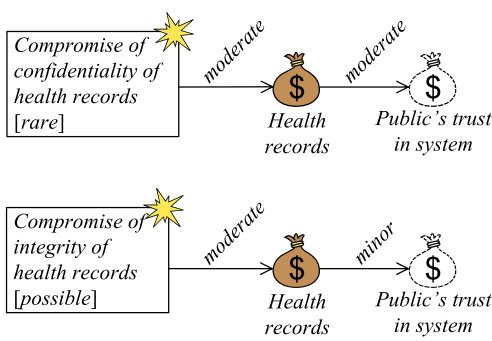
The risk evaluation furthermore includes the estimation and evaluation of the risks with respect to the indirect assets. Because the indirect assets are harmed only through harm to the direct assets, the relevant unwanted incidents with likelihoods are already identified. What remains is to determine the consequence of the harm to the direct assets on the related indirect assets. For the purpose of this, we need to define a consequence scale for each of the indirect assets, and we need to define their risk evaluation criteria.

*Example 3.7* The analysis leader shows the asset diagram of Fig. 3.7 and explains that every risk with respect to the direct assets *Provision of telecardiology service* and *Health records* may represent a risk with respect to the indirect asset *Public's trust in system*. A consequence scale similar to the one in Table 3.4 with values ranging from *insignificant* to *catastrophic* is defined. The customer furthermore decides to use the risk evaluation criteria defined in Table 3.5 also for the indirect asset.

Each unwanted incident that harms one or both of the two relevant direct assets represents a risk with respect to the indirect asset. The analysis leader presents each of the relevant unwanted incidents in turn in order to have the participants to decide the consequence for the indirect asset. Figure 3.13 shows the consequence estimations for two of the unwanted incidents. The analysis leader explains that the full documentation of the risks with respect to the indirect asset is already given in the threat diagrams for the direct assets.

Once all the relevant unwanted incidents have been identified, and their likelihoods as well as consequences for both direct and indirect assets have been estimated, we are ready to evaluate the risks.

**Fig. 3.13** Harm to indirect assets



**Table 3.7** Risk evaluation matrix with risks

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare			CC1, CC1(I)		
	Unlikely					PR1
	Possible		CI1(I), SS1(I)	CI1, SS1		
	Likely				SS2	
	Certain					

*Example 3.8* In this case, the risks are evaluated by plotting them into the risk evaluation matrix. From the five unwanted incidents in the threat diagram, the analysis secretary extracts five risks with respect to the direct assets. *CC1: Compromise of confidentiality of health records*, which may affect health records. *CI1: Compromise of integrity of health records*, which may also harm health records. The latter may also lead to the risk *PR1: Patient is given wrong diagnosis*, which may harm the patient’s health. *SS1: Slow system* may affect the provisioning of the telecardiology system, and also lead to the risk *SS2: Unable to set diagnosis due to slow system*, which may affect the patients’ health. Only *CC1* is within acceptable risk level; the remaining risks need further evaluation.

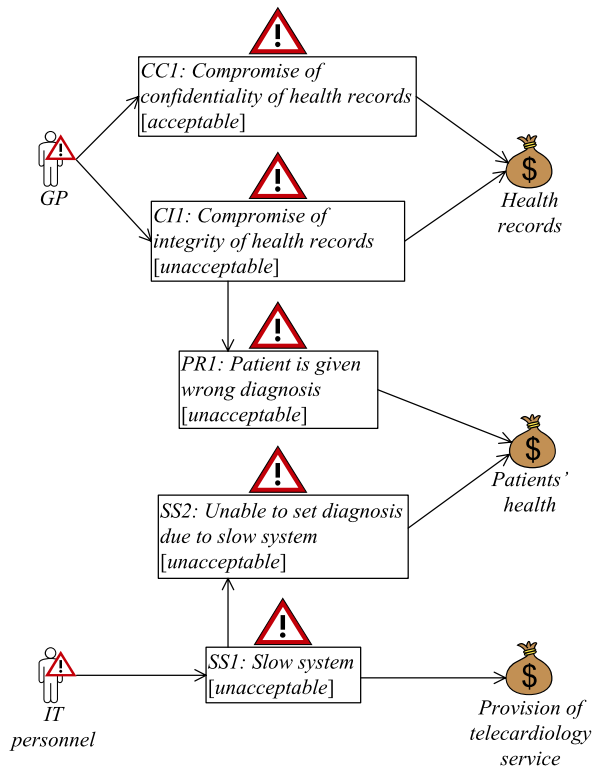
Three of the unwanted incidents in Fig. 3.12 moreover represent risks with respect to the indirect asset. The risk *CC1(I): Compromise of confidentiality of health records* may affect *Public’s trust in system*, and the analysis secretary uses the suffix (*I*) to convey that the risk is with respect to the indirect asset. The other risks with respect to the indirect asset are named by the same convention.

Table 3.7 positions the risks within the risk evaluation matrix. The customer is at this point also invited to reconsider the risks to the indirect asset based on the risks to the direct assets, but our customer is now of the opinion that it is sufficient to focus on the direct ones in this particular analysis.

The analysis leader invites the customer to adjust likelihood and consequence estimates, as well as risk evaluation levels, to make sure that the results reflect reality as much as possible.

The participants request an overview of the risks. They want to know who or what is initiating them and which assets they harm. In response the analysis leader presents the risks, including the risks with respect to the indirect assets, with their associated risk values in terms of CORAS risk diagrams. The final diagram regarding

Fig. 3.14 Risk diagram

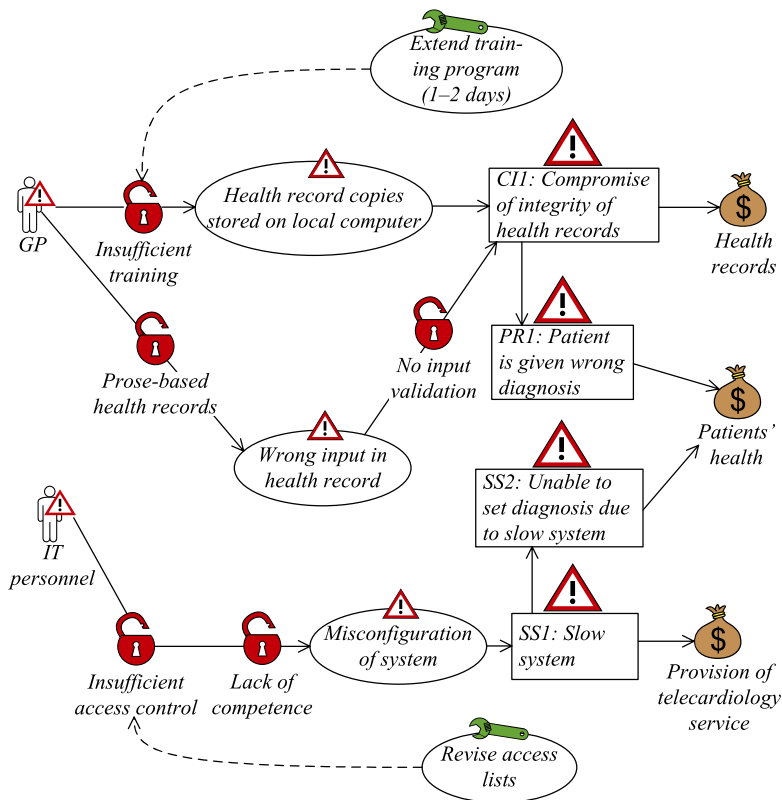


the direct assets for risks accidentally caused by employees is shown in Fig. 3.14. Since the *CC1* is within the acceptable risk level it will not be considered in the treatment phase of Step 8 of the CORAS method. The same is the case for the risks with respect to the indirect assets.

### 3.8 Risk Treatment Using Treatment Diagrams

Step 8 is devoted to treatment identification, as well as addressing cost-benefit issues of the treatments. A main task of Step 8 is the treatment identification using CORAS treatment diagrams, which is also often organised as a workshop. The risks that are not acceptable are all addressed in order to find means to reduce their likelihood and/or consequence. Since treatments can be costly, they are assessed with respect to cost-benefit, before a final treatment plan is made. The initial treatment diagrams are similar to the final threat diagrams except that unwanted incidents are replaced by the risks from the risk diagram.

*Example 3.9* The analysis leader presents preliminary treatment diagrams showing all the unacceptable risks, ready to be filled in with treatments. He knows that



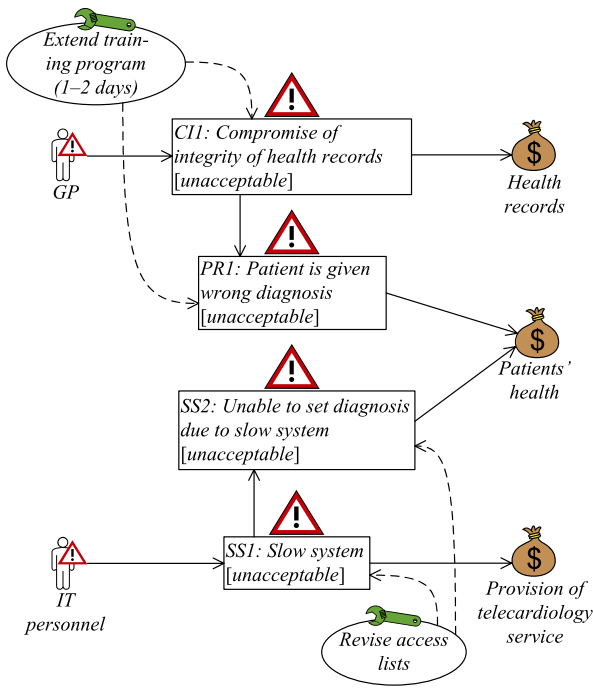
**Fig. 3.15** Treatment diagram

participants of analyses often find it most intuitive to address vulnerabilities when looking for treatments. Hence, he highlights the possibility of treating other parts of the target as well, such as threats or threat scenarios. The participants involve in a discussion of potential treatments, and decide which ones will reduce the risks to acceptable levels. On some occasions, when the discussion gets slightly out of scope, the analysis leader suggests treatments taken from best-practice descriptions for network solutions and cryptography to help the discussion back on track. The diagrams are annotated with the identified treatment options indicating where they will be implemented. Finally, the following treatments are suggested and annotated in the treatment diagram of Fig. 3.15:

- Extend the training program for practitioners with 1–2 days, with a special focus on security aspects.
- Revise the list of people having access to conduct maintenance.

When the final results from the analysis are presented to the customer, an overview of the risks and the proposed treatments is useful. In our case, the treatment overview diagram of Fig. 3.16 is used for this purpose.

**Fig. 3.16** Treatment overview diagram





<http://www.springer.com/978-3-642-12322-1>

Model-Driven Risk Analysis

The CORAS Approach

Lund, M.S.; Solhaug, B.; Stolen, K.

2011, XVI, 460 p., Hardcover

ISBN: 978-3-642-12322-1