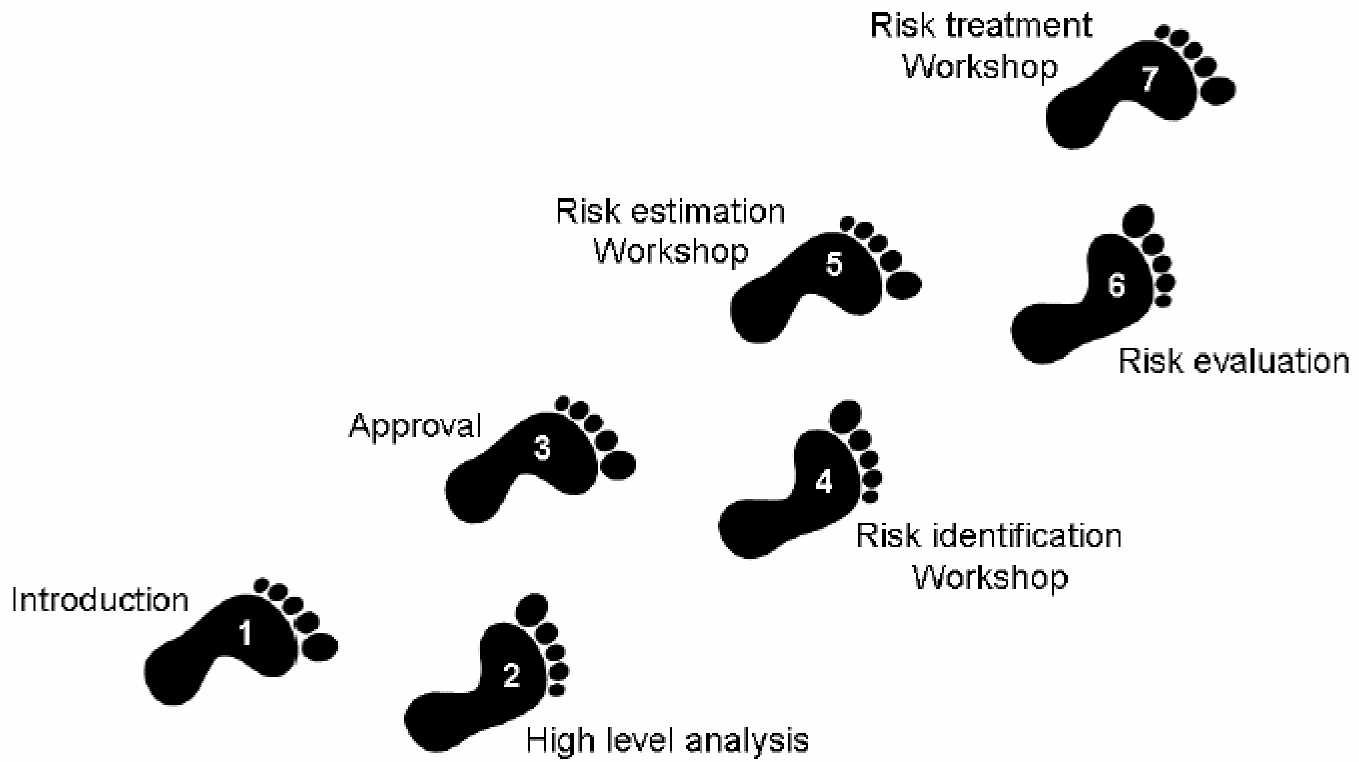
Security analysis:
CORAS in seven steps

November 17, 2006

Ketil Stølen, SINTEF & UiO

The seven steps of a security analysis in CORAS



Step 1: Introduction

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

Tasks

- The security analysis method is introduced.
- The client presents the goals and the target of the analysis.
- The focus and scope of the analysis is set.
- The meetings and workshops are planned.

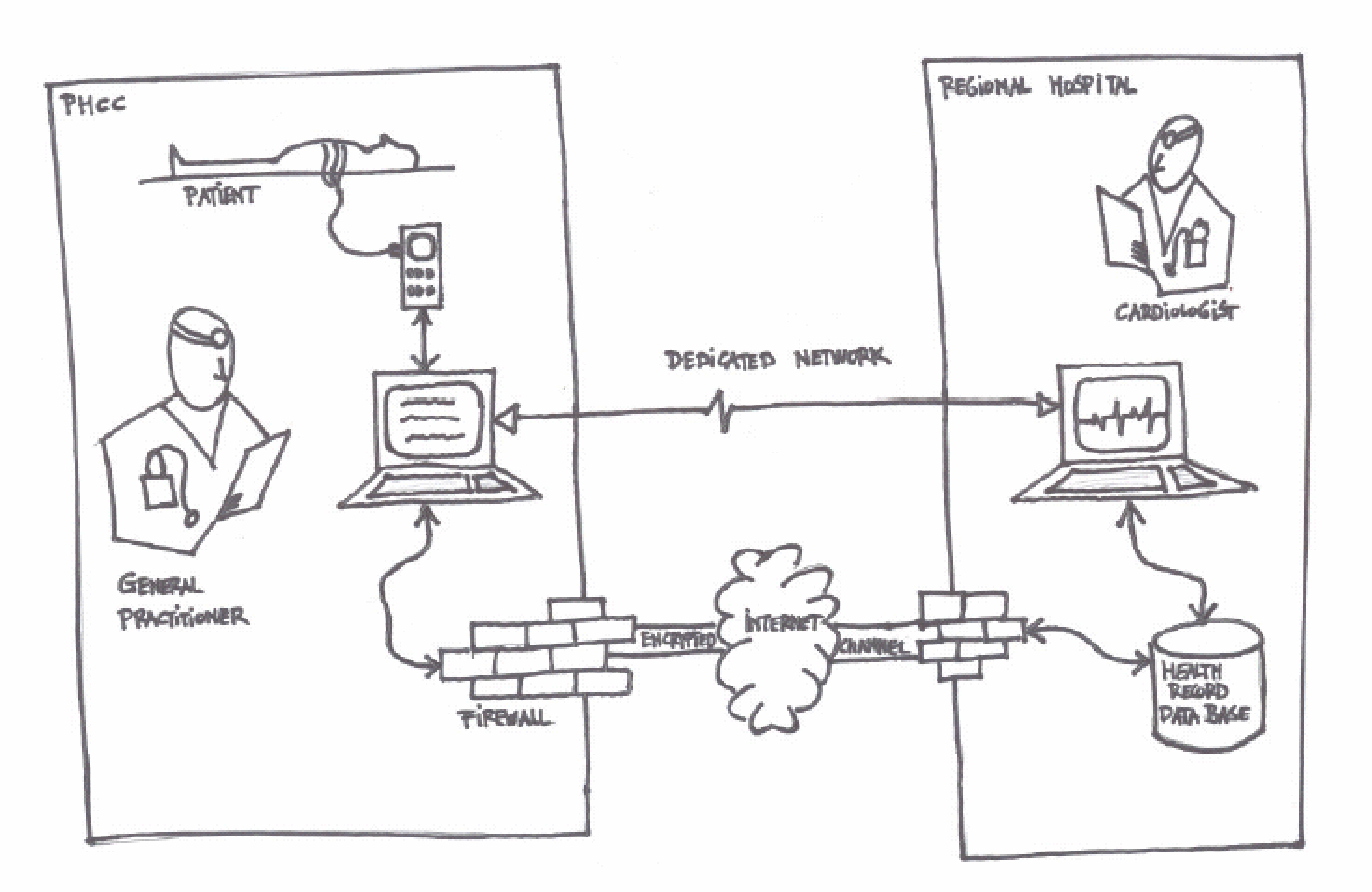
People that should participate

- Analysis leader (required)
- Analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise (optional)
  - Users (optional)

Modelling guideline

- At this early stage of the analysis it can be useful to describe the target with informal like drawings, pictures or sketches on a blackboard.
- The presentation can later be supplemented with more formal modelling techniques such as UML or data flow-diagram.

Telemedicine case



Step 2: High level analysis

- The second step also involves a separate meeting with representatives of the client.
- However, this time the analysts will present their understanding of what they learned at the rst meeting and from studying documentation that has been made available to them by the client.
- The second step also involves a rough, high-level security analysis.
- During this analysis the first threats, vulnerabilities, threat scenarios and unwanted incidents are identied.
- They will be used to help directing and scoping the more detailed analysis still to come.

Tasks

- The target as understood by the analysts is presented.
- The assets are identied.
- A high-level analysis is conducted.

People that should participate

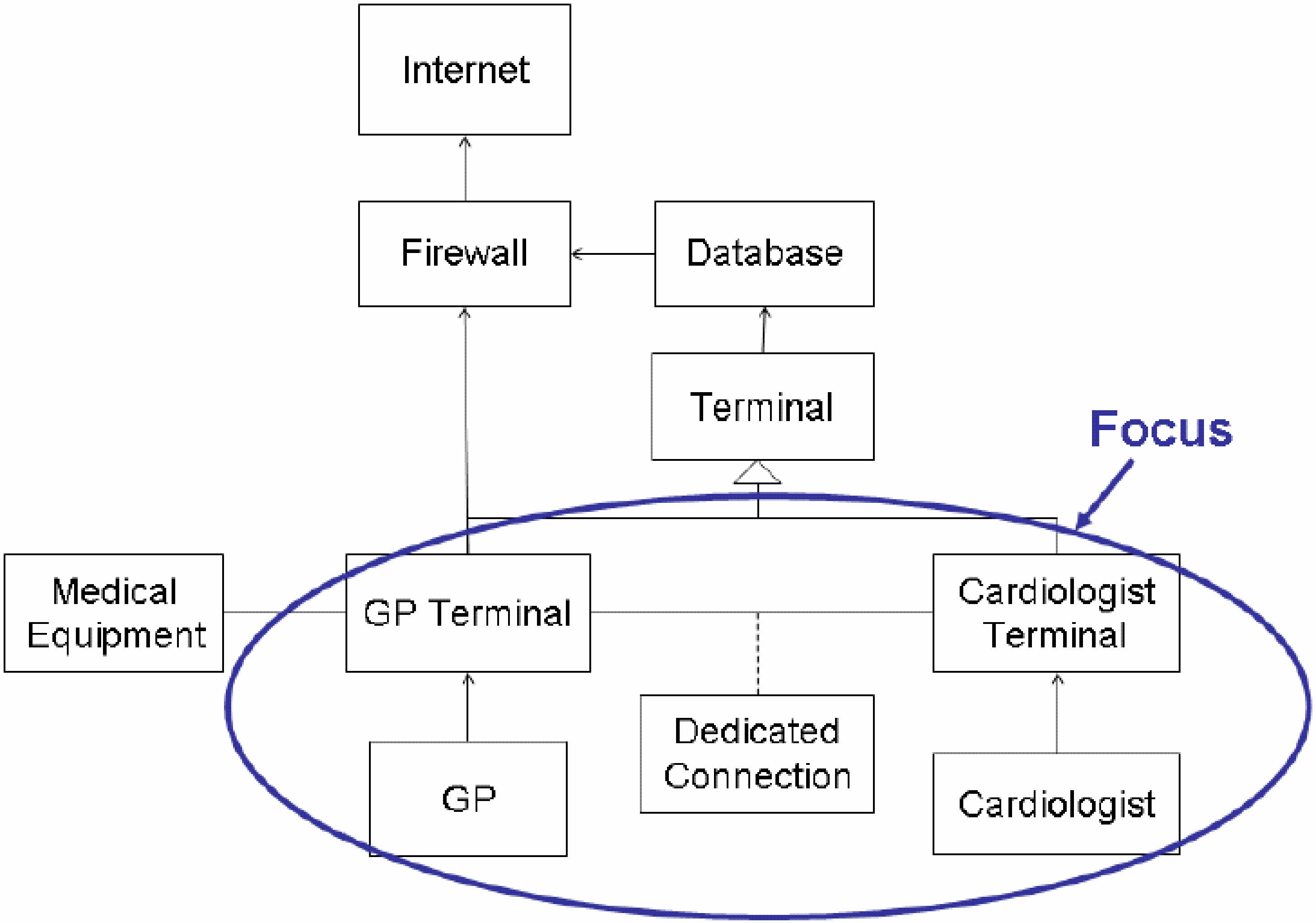
- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise (required)
  - Users (optional)

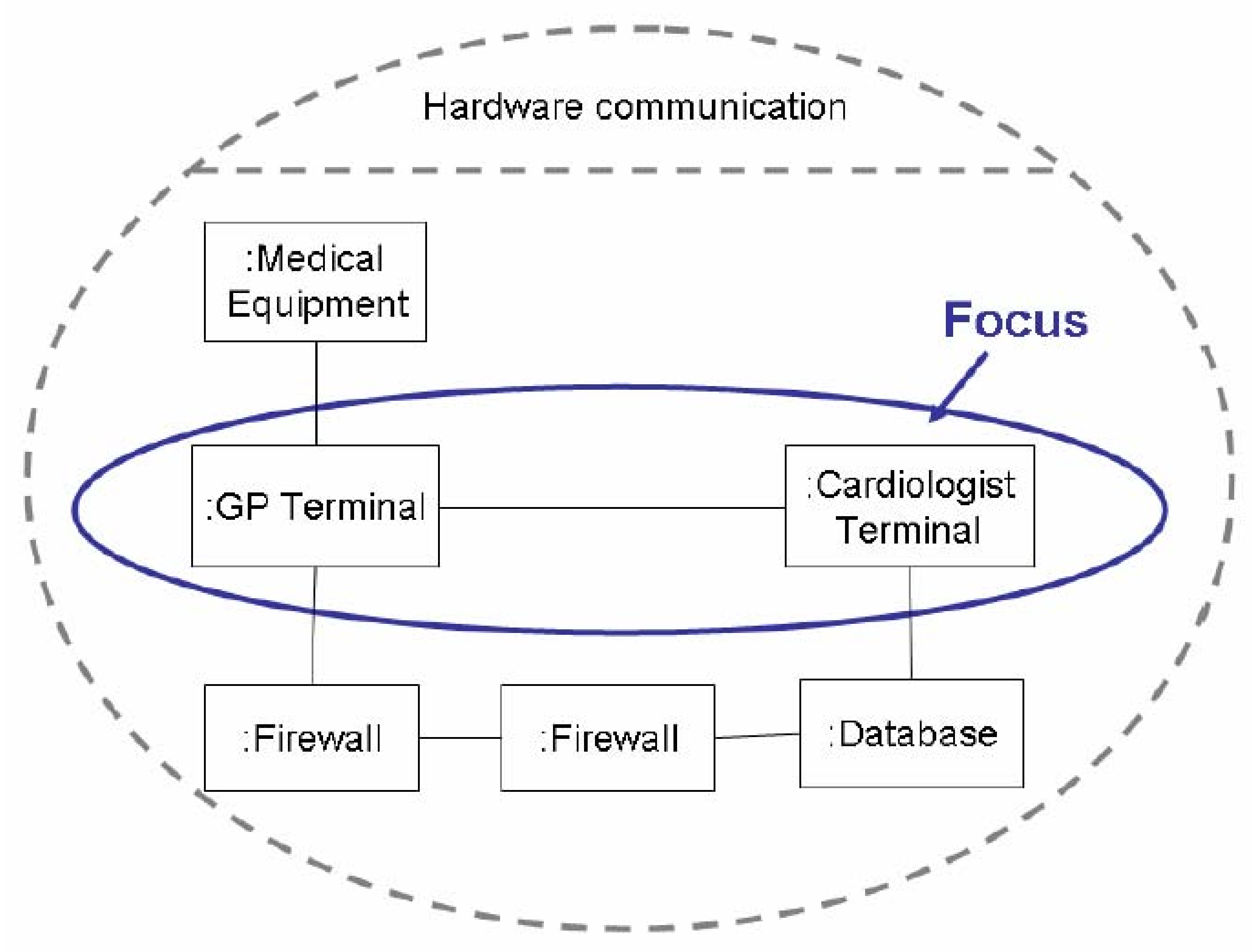
Modelling guideline for the target description

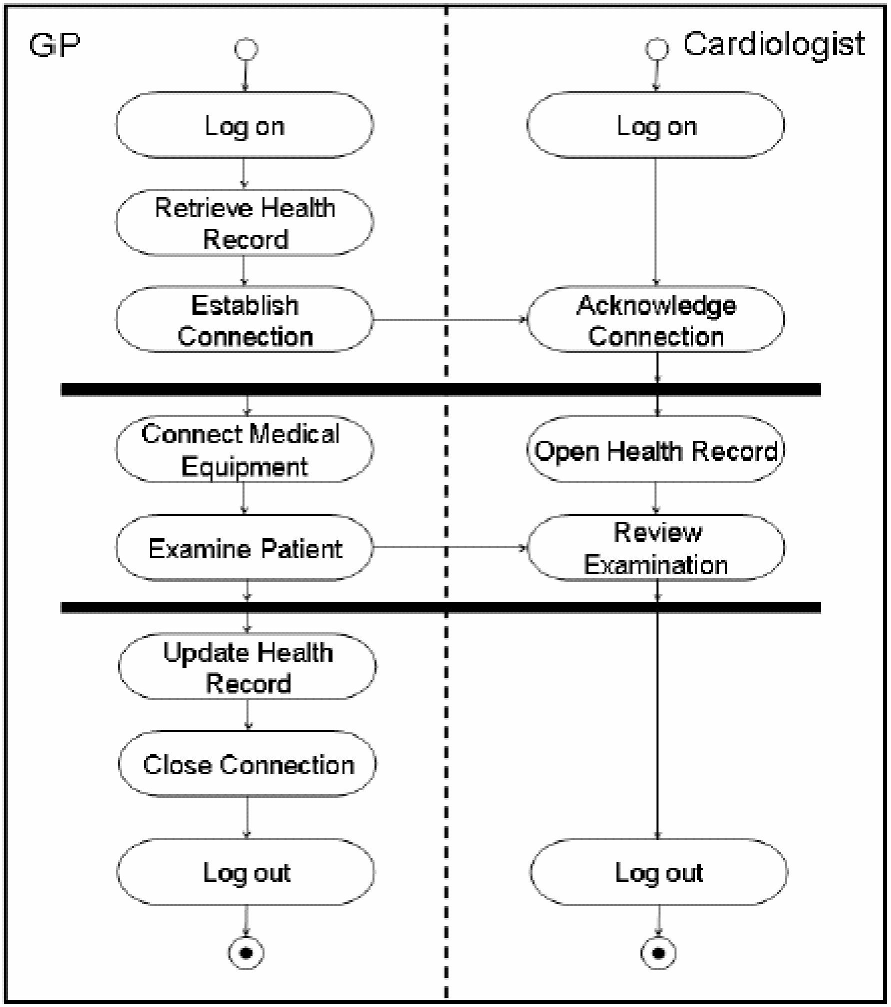
- Use a formal or standardised notation such as UML, but ensure that the notation is explained thoroughly so that the participants understand it.
- Create models of both the static and the dynamic features of the target.
- Static may be hardware congurations, network design etc., while dynamic may be work processes, information ow etc.
- For the static parts of the description UML class diagrams and UML
- collaboration diagrams (or similar notations) are recommended.
- For the dynamic parts we recommend UML activity diagrams and
- UML sequence diagrams (or similar notations)

Modelling guideline for asset diagrams

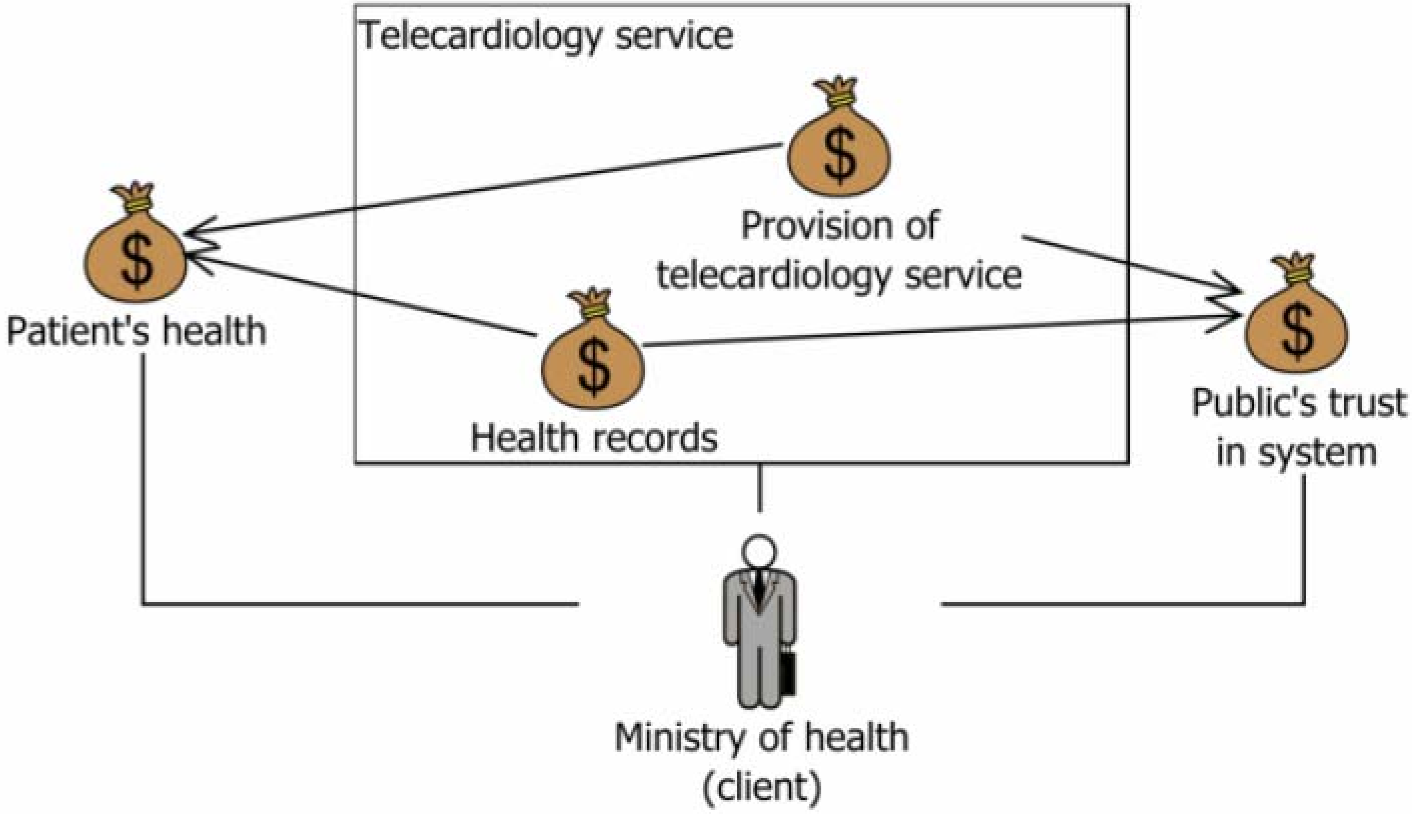
- Draw a region that logically or physically represents the target of analysis.
- Place the direct assets within the region.
- Place the indirect assets outside the region. Indirect assets are a harmed as a consequence of a direct asset being harmed first.
- Indicate with arrows how assets may affect other assets.
- Assets may be ranked according to their importance.
- If the analysis has more than one client, the clients should be associated with their assets.


Internet
Firewall
Database
Terminal
Focus
Medical Equipment
GP Terminal
Cardiologist Terminal
Dedicated Connection
GP
Cardiologist

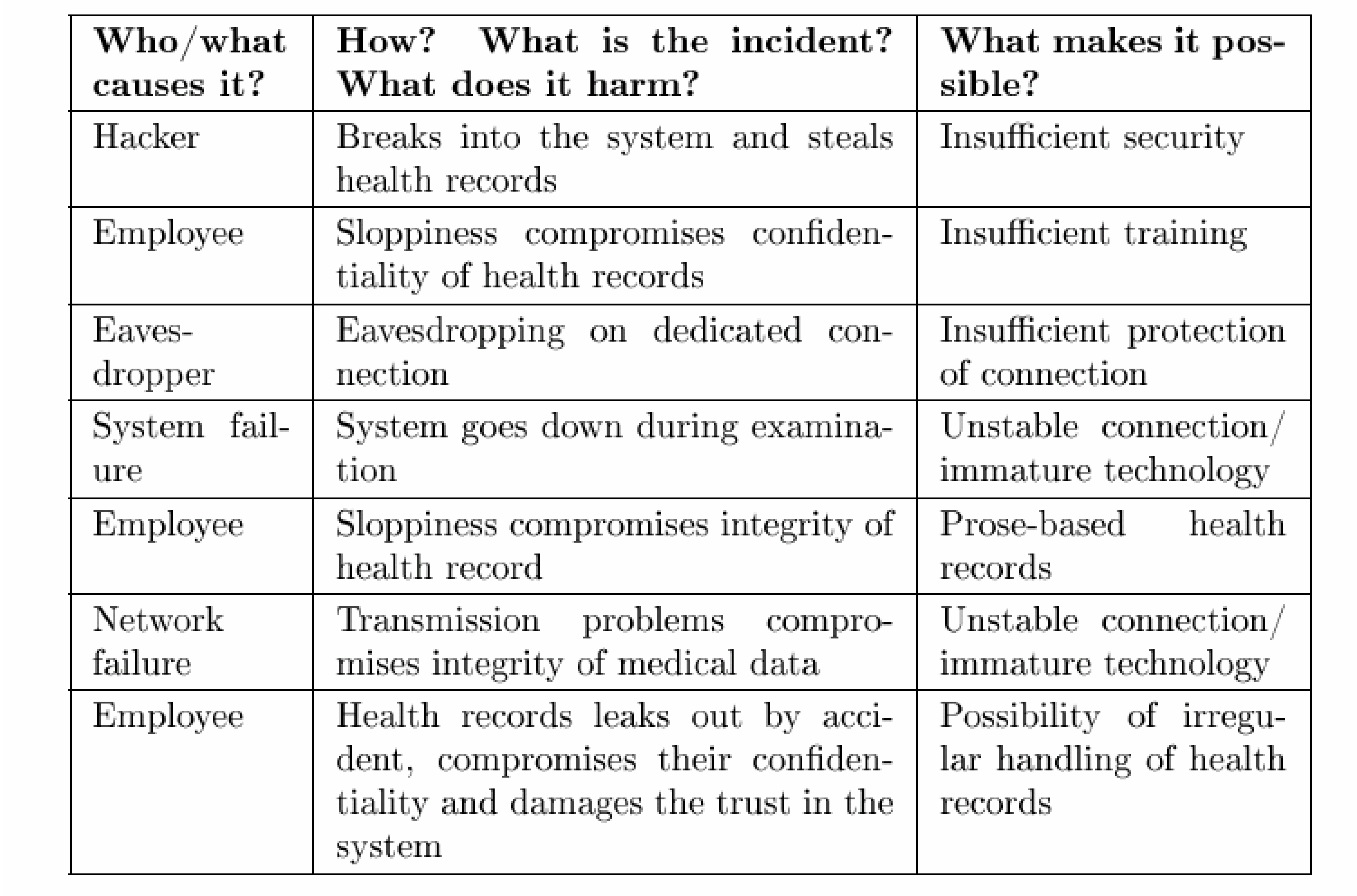

Hardware communication
:Medical Equipment
Focus
:GP Terminal
:Cardiologist Terminal
:Firewall
:Firewall
:Database


GP
Cardiologist
Log on
Log on
Retrieve Health Record
Establish Connection
Acknowledge Connection
Connect Medical Equipment
Open Health Record
Examine Patient
Review Examination
Update Health Record
Close Connection
Log out
Log out

Asset diagram



High-level risk table



Who/what causes it?	How? What is the incident? What does it harm?	What makes it possible?
Hacker	Breaks into the system and steals health records	Insufficient security
Employee	Sloppiness compromises confidentiality of health records	Insufficient training
Eavesdropper	Eavesdropping on dedicated connection	Insufficient protection of connection
System failure	System goes down during examination	Unstable connection/ immature technology
Employee	Sloppiness compromises integrity of health record	Prose-based health records
Network failure	Transmission problems compromises integrity of medical data	Unstable connection/ immature technology
Employee	Health records leaks out by accident, compromises their confidentiality and damages the trust in the system	Possibility of irregular handling of health records

Step 3: Approval

- The third step involves a more refined description of the target to be analysed, and also
  - all assumptions being made and
  - other preconditions made.
- Step three is terminated once all this documentation has been approved by the client.

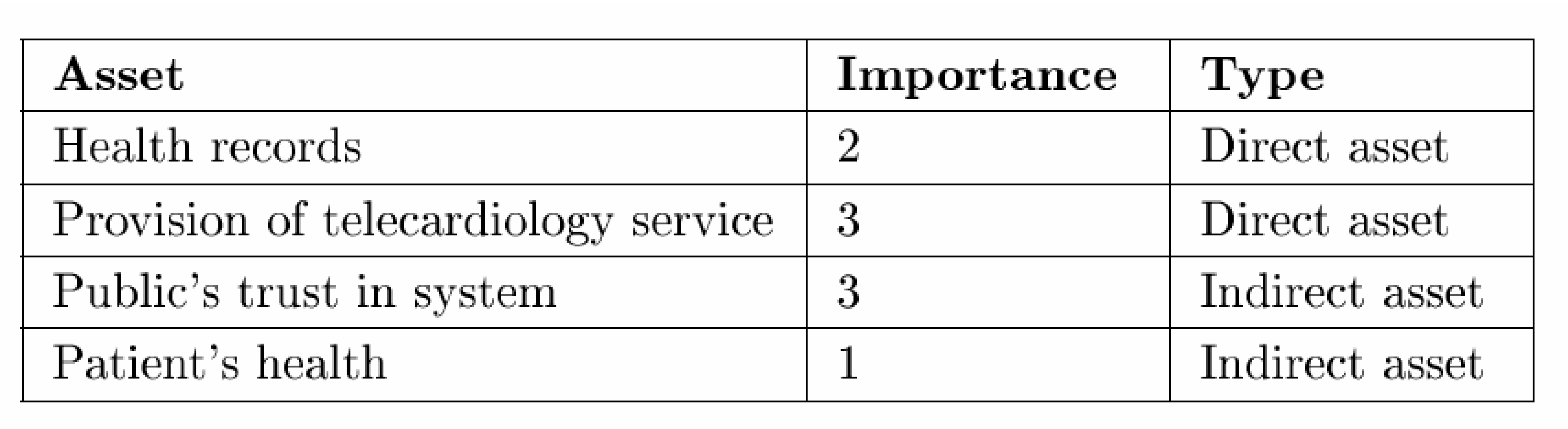
Tasks

- The client approves target descriptions and asset descriptions.
- The assets should be ranked according to importance.
- Consequence scales must be set for each asset within the scope of the analysis.
- A likelihood scale must be defined.
- The client must decide risk evaluation criteria for each asset within the scope of the analysis.

People that should participate

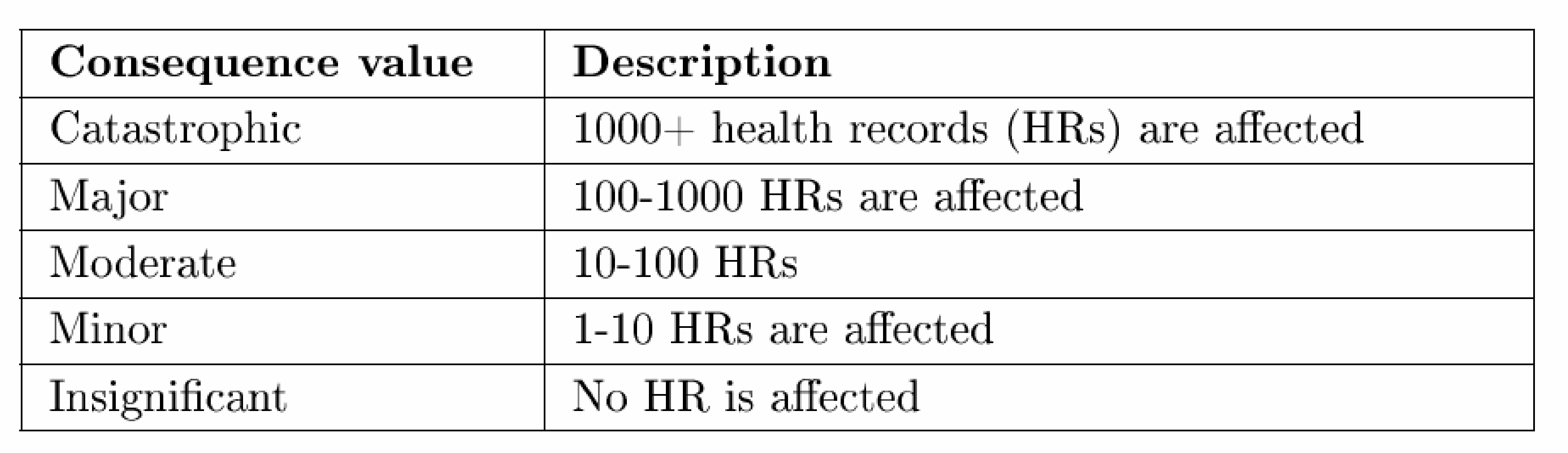
- The same as in the previous meeting, but since this step sets the boundaries for the further analysis it is important that the relevant decision-makers are present.

Asset table



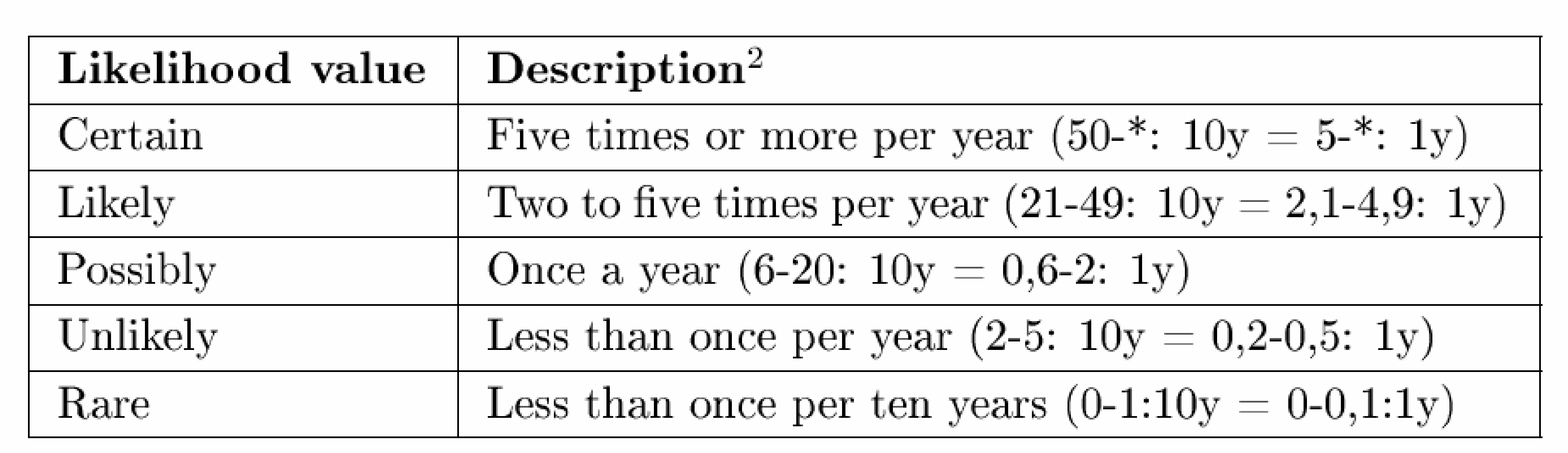
Asset	Importance	Type
Health records	2	Direct asset
Provision of telecardiology service	3	Direct asset
Public's trust in system	3	Indirect asset
Patient's health	1	Indirect asset

Consequence scale for ”health records”



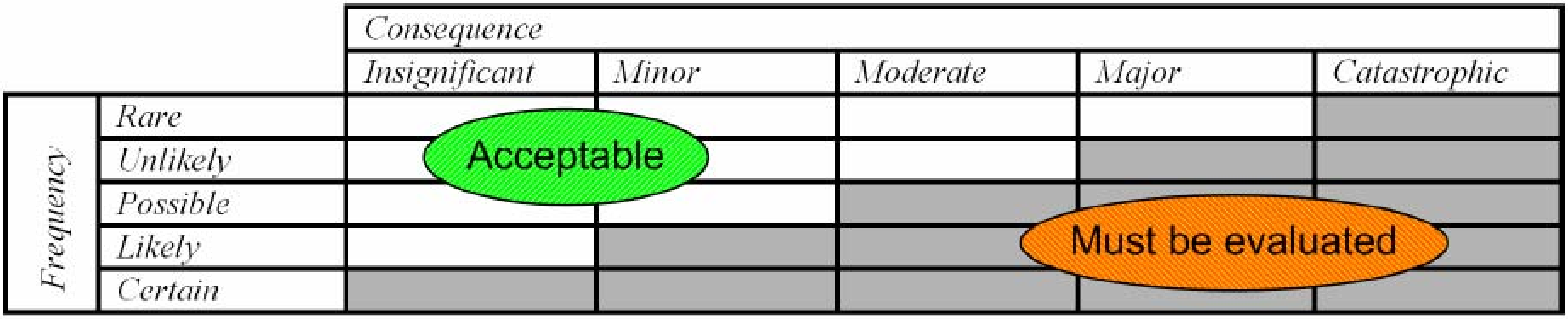
Consequence value	Description
Catastrophic	1000+ health records (HRs) are affected
Major	100-1000 HRs are affected
Moderate	10-100 HRs
Minor	1-10 HRs are affected
Insignificant	No HR is affected

Likelihood scale



Likelihood value	Description[2]
Certain	Five times or more per year (50-*: 10y = 5-*: 1y)
Likely	Two to five times per year (21-49: 10y = 2,1-4,9: 1y)
Possibly	Once a year (6-20: 10y = 0,6-2: 1y)
Unlikely	Less than once per year (2-5: 10y = 0,2-0,5: 1y)
Rare	Less than once per ten years (0-1:10y = 0-0,1:1y)

Risk evaluation matrix



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

Acceptable

Must be evaluated

Step 4: Risk identification workshop

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

Tasks

- The initial threat diagrams should be completed with identied threats, vulnerabilities, threat scenarios and unwanted incidents.

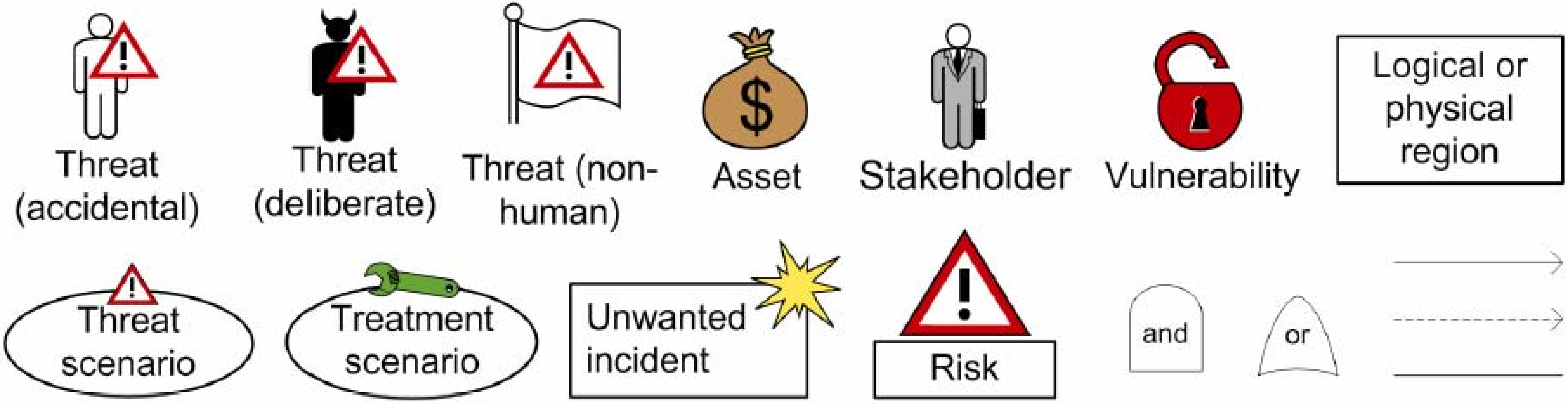
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (optional)
  - Technical expertise (required)
  - Users (required)

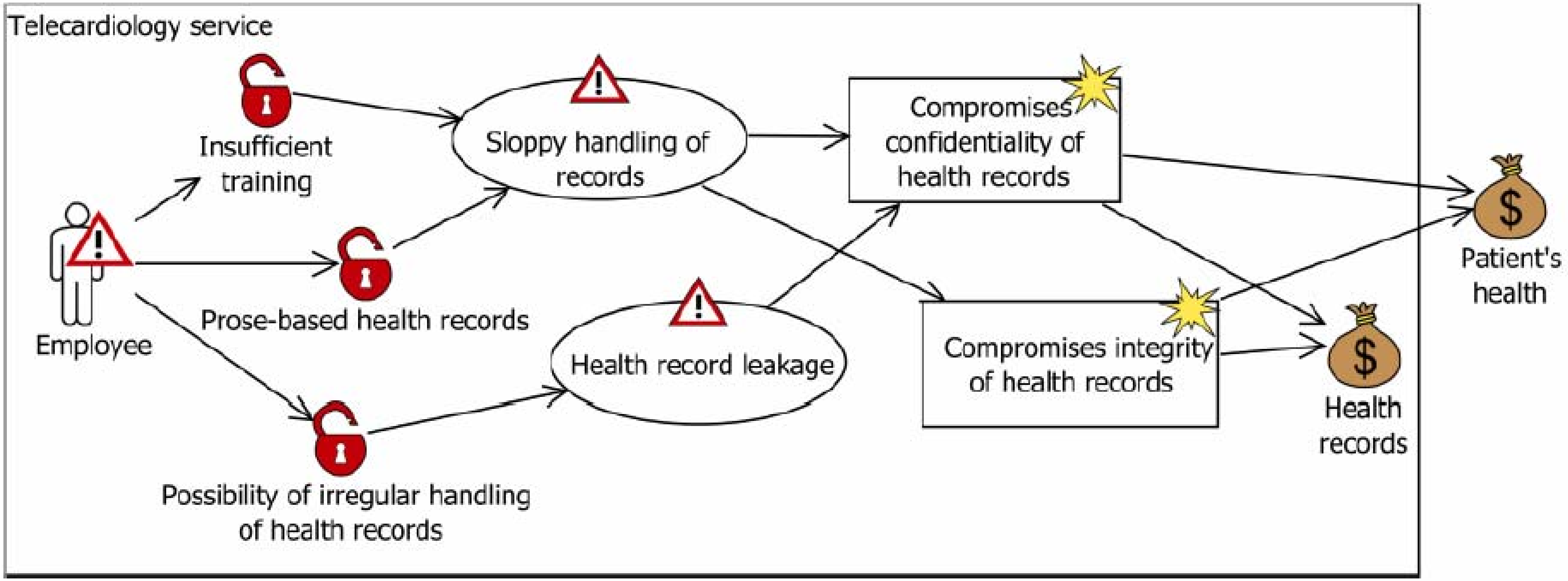
Modelling guideline for threat diagrams

- Use the region from the asset diagram and add more regions if necessary.
- Model different kinds of threats in separate diagrams.
- Assets are listed to the right, outside the region.
- Threats are placed to the left in the region; threats that can be classified as external are placed outside the region.
- Unwanted incidents are placed within the region with relations to the assets they impact.
- Assets that are not harmed by any incidents are removed from the diagram.
- Add threat scenarios between the threats and the unwanted incidents in the same order as they occur in real time (i.e. in a logical sequence).
- Insert the vulnerabilities before the threat scenario or unwanted incident they lead to.

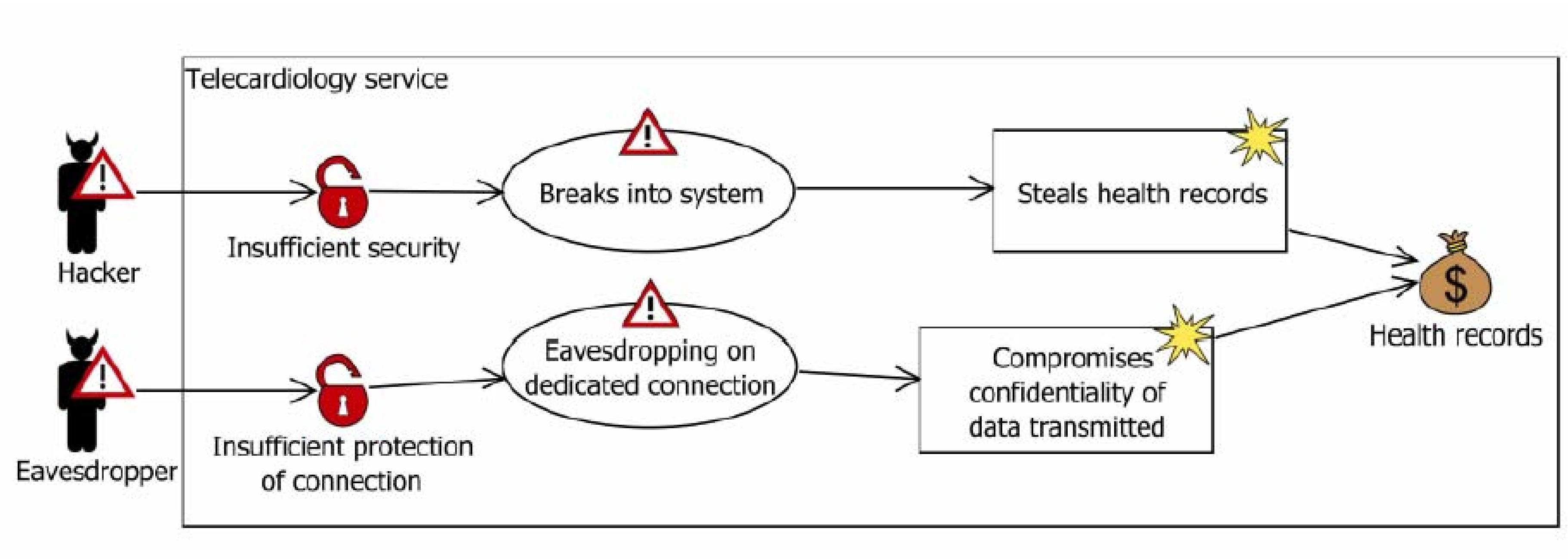
Symbols from the CORAS risk modelling language



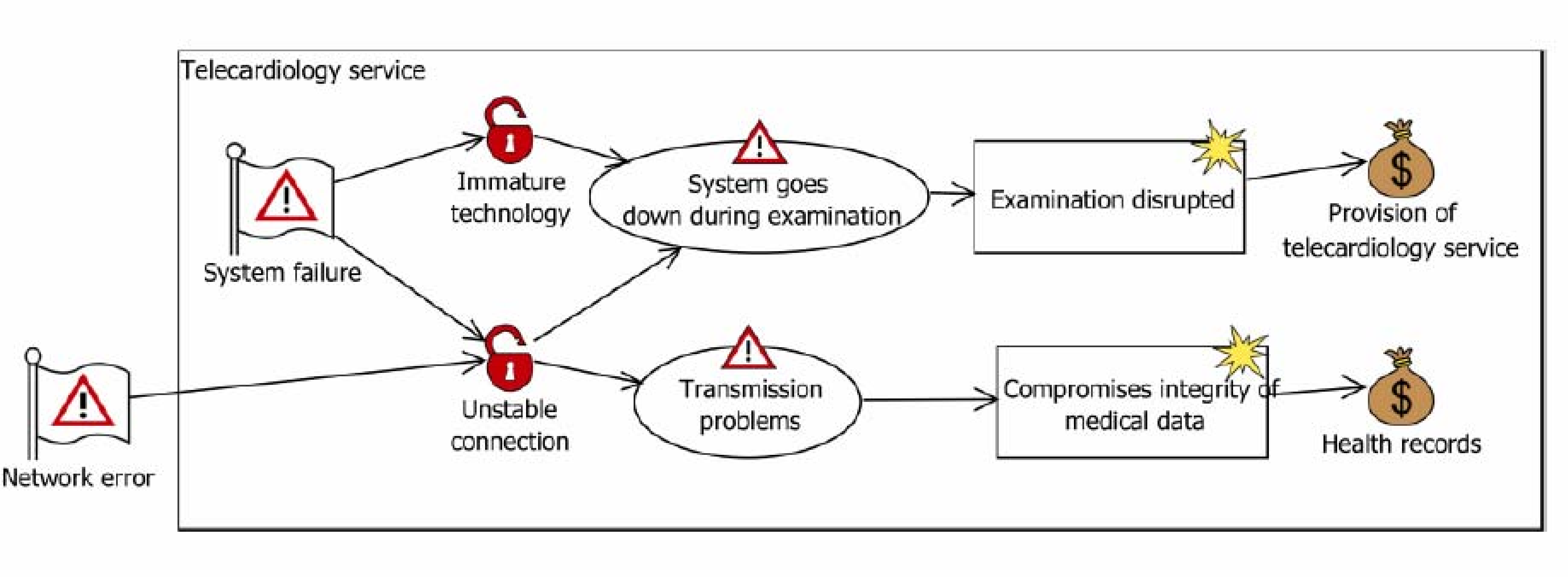
Initial threat diagram: accidental actions


Telecardiology service
Insufficient training
Sloppy handling of records
Compromises confidentiality of health records
Employee
Prose-based health records
Health record leakage
Compromises integrity of health records
Patient's health
Health records
Possibility of irregular handling of health records

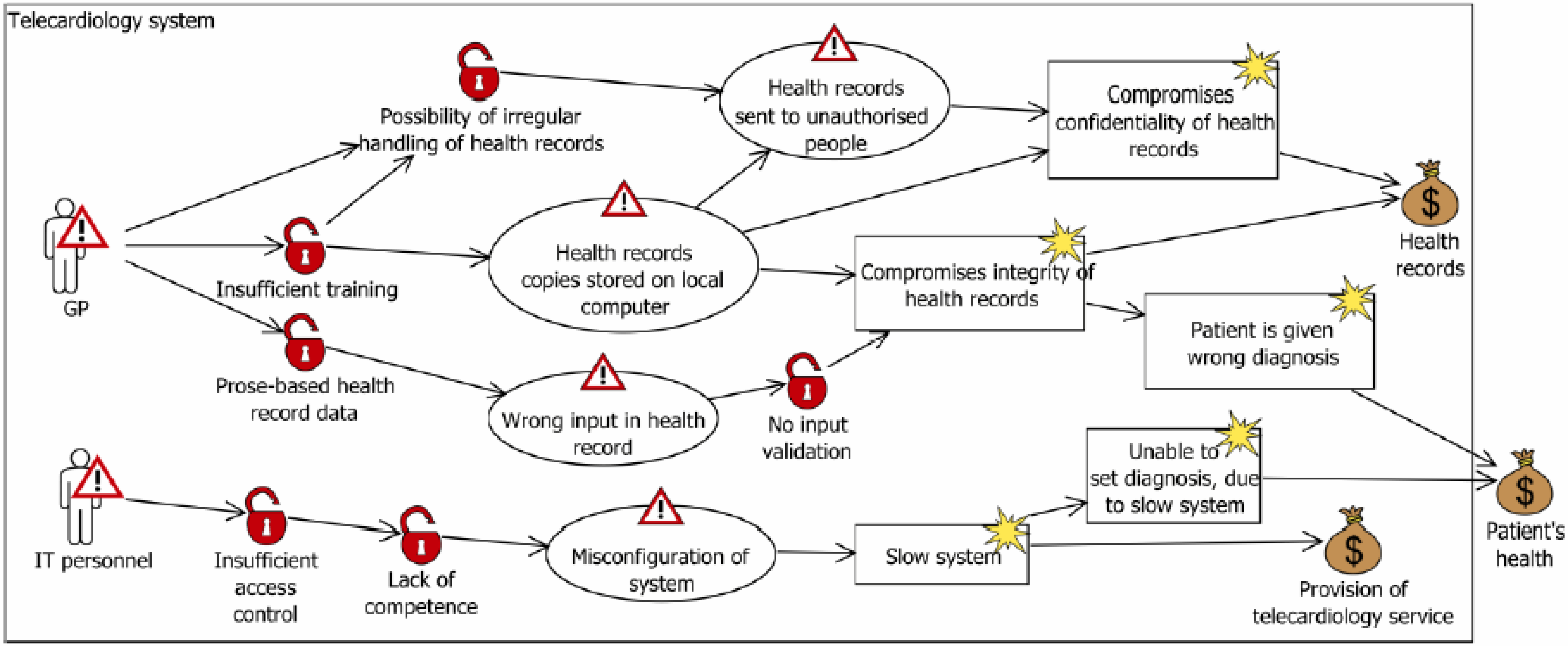
Initial threat diagram: deliberate actions


Telecardiology service
Hacker
Insufficient security
Breaks into system
Steals health records
Health records
Eavesdropper
Insufficient protection of connection
Eavesdropping on dedicated connection
Compromises confidentiality of data transmitted

Initial threat diagram: non-human threats



Final threat diagram: accidental actions


Telecardiology system
Possibility of irregular handling of health records
Health records sent to unauthorised people
Compromises confidentiality of health records
GP
Insufficient training
Health records copies stored on local computer
Compromises integrity of health records
Health records
Prose-based health record data
Wrong input in health record
No input validation
Patient is given wrong diagnosis
IT personnel
Insufficient access control
Lack of competence
Misconfiguration of system
Slow system
Unable to set diagnosis, due to slow system
Patient's health
Provision of telecardiology service

Step 5: Risk Estimation Workshop

- The fifth step is also organised as a workshop.
- This time with focus on estimating consequences and likelihood values for each of the identified unwanted incidents.

Tasks

- Every threat scenario must be given a likelihood estimate and unwanted incident likelihoods are based on these.
- Every relation between an unwanted incident and an asset must be given a consequence estimate.

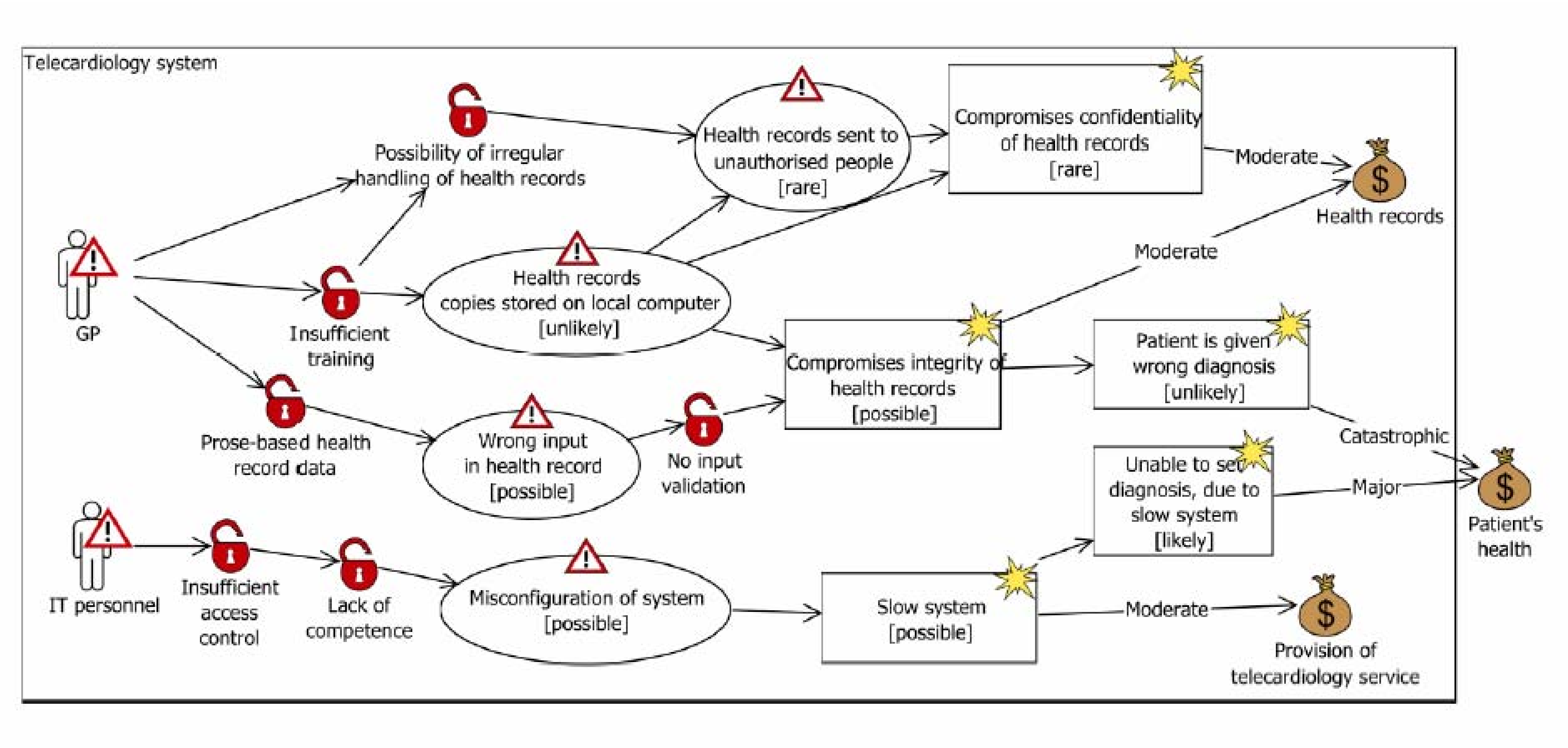
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise regarding the target (required)
  - Users (required)

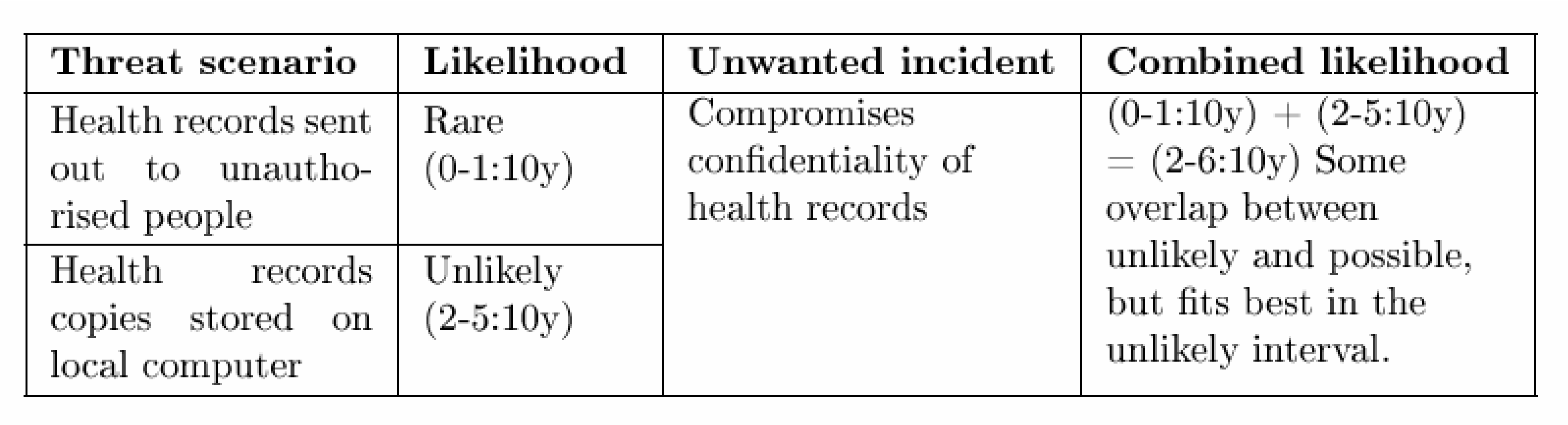
Modelling guideline

- Risk estimation on threat diagrams:
  - Add likelihood estimates to the threat scenarios.
  - Add likelihood estimates to the unwanted incidents, based on the threat scenarios.
  - Annotate each unwanted incident-asset relation with a consequence taken from the respective asset's consequence scale.

Threat diagram with likelihood and consequence estimates


Telecardiology system
GP
IT personnel
Possibility of irregular handling of health records
Insufficient training
Prose-based health record data
Health records sent to unauthorised people [rare]
Health records copies stored on local computer [unlikely]
Wrong input in health record [possible]
No input validation
Insufficient access control
Lack of competence
Misconfiguration of system [possible]
Compromises confidentiality of health records [rare]
Compromises integrity of health records [possible]
Patient is given wrong diagnosis [unlikely]
Unable to set diagnosis, due to slow system [likely]
Slow system [possible]
Moderate
Moderate
Catastrophic
Major
Moderate
Health records
Patient's health
Provision of telecardiology service

Combined likelihood estimates



Threat scenario	Likelihood	Unwanted incident	Combined likelihood
Health records sent out to unauthorised people	Rare (0-1:10y)	Compromises confidentiality of health records	(0-1:10y) + (2-5:10y) = (2-6:10y) Some overlap between unlikely and possible, but fits best in the unlikely interval.
Health records copies stored on local computer	Unlikely (2-5:10y)		

Step 6: Risk Evaluation

- This step involves giving the client the first overall risk picture.
- This will typically trigger some adjustments and corrections.

Tasks

- Likelihood and consequence estimates should be confirmed or adjusted.
- The final adjustments of the acceptable area in the risk matrices should be made (if needed).
- An overview of the risks may be given in a risk diagram.

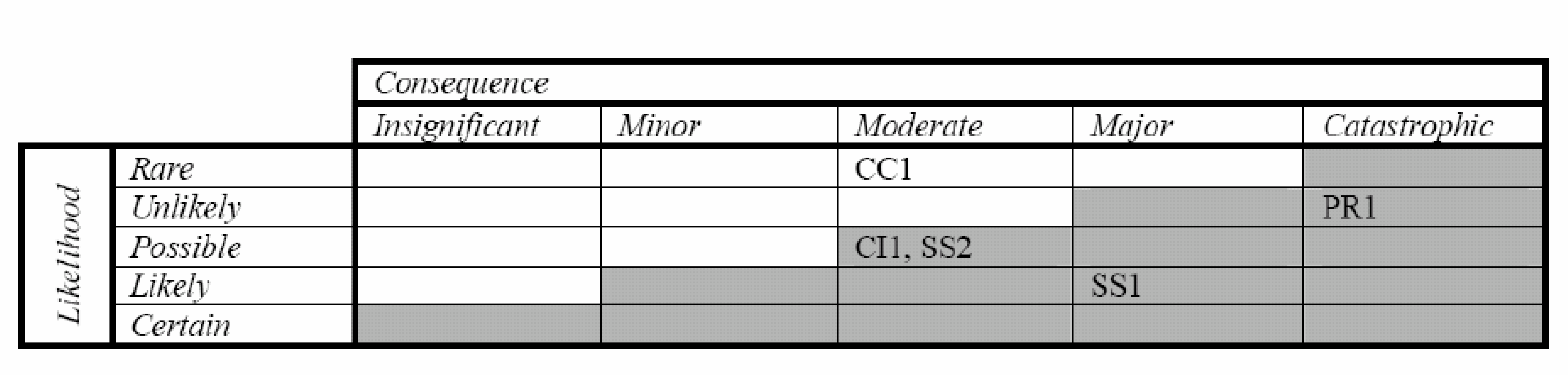
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise regarding the target (optional)
  - Users (optional)

Modelling guideline for risk diagrams

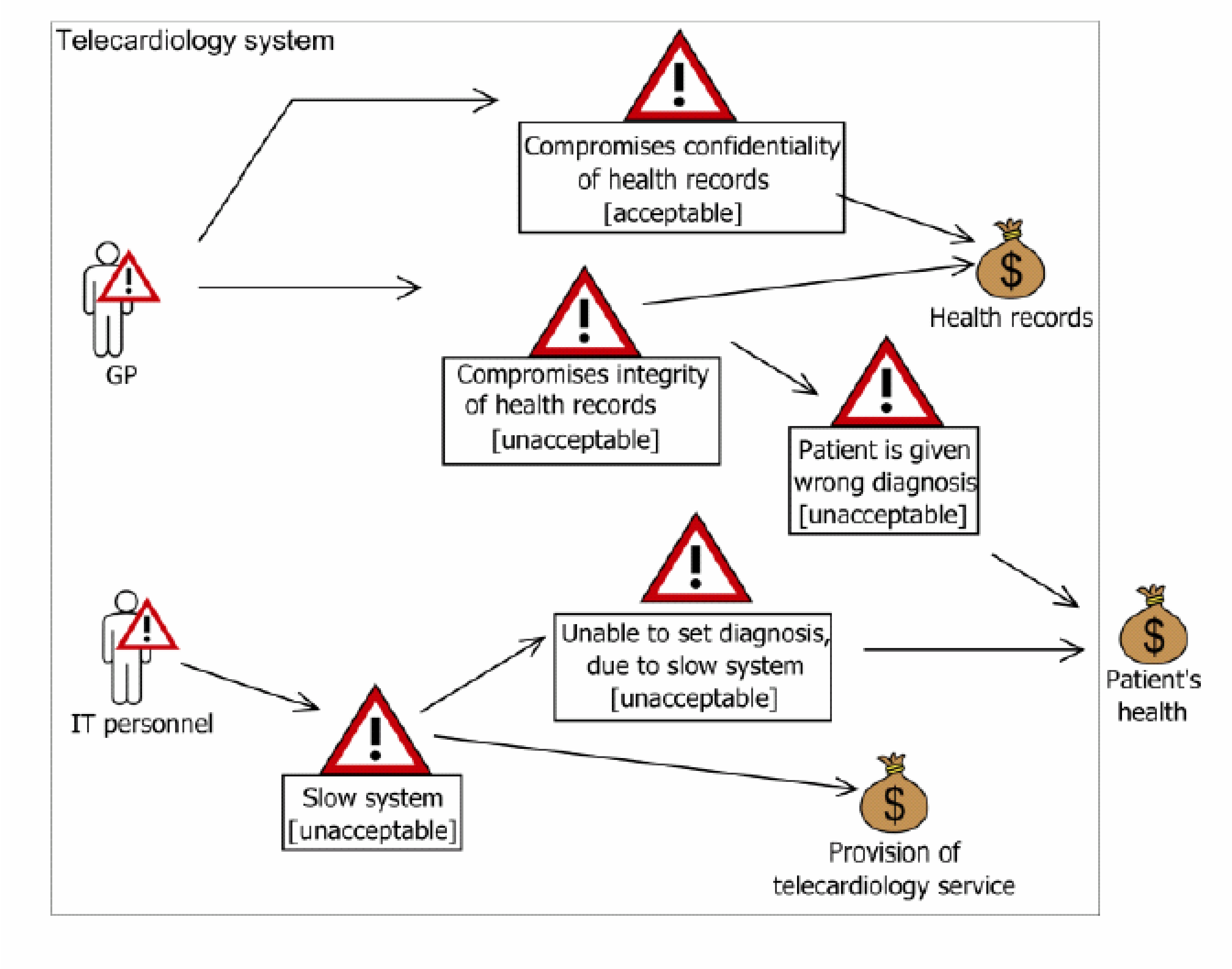
- Use the threat diagram and replace all unwanted incidents with risk symbols, showing a short risk description and whether the risk is acceptable or not.
- Remove threat scenarios and vulnerabilities, but keep the relations between the threats and the risks.
- If useful, split the risk diagrams into several diagrams according to type of threat, part of the target or asset importance (e.g. show all risks related to network, all risks for specic assets etc.).

Risk evaluation matrix with risks



		Consequence				
		Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Likelihood	*Rare*			CC1		
	Unlikely					PR1
	Possible			CI1, SS2		
	Likely				SS1	
	Certain					

Risk overview diagram


Telecardiology system
Compromises confidentiality of health records [acceptable]
GP
Compromises integrity of health records [unacceptable]
Health records
Patient is given wrong diagnosis [unacceptable]
Unable to set diagnosis, due to slow system [unacceptable]
Patient's health
IT personnel
Slow system [unacceptable]
Provision of telecardiology service

Step 7: Risk treatment workshop

- The last step is devoted to treatment identication, as well as addressing cost/benefit issues of the treatments.
- This step is best organised as a workshop.

Tasks

- Add treatments to threat diagrams.
- Estimate the cost/benet of each treatment and decide which ones to use.
- Show treatments in risk overview diagrams.

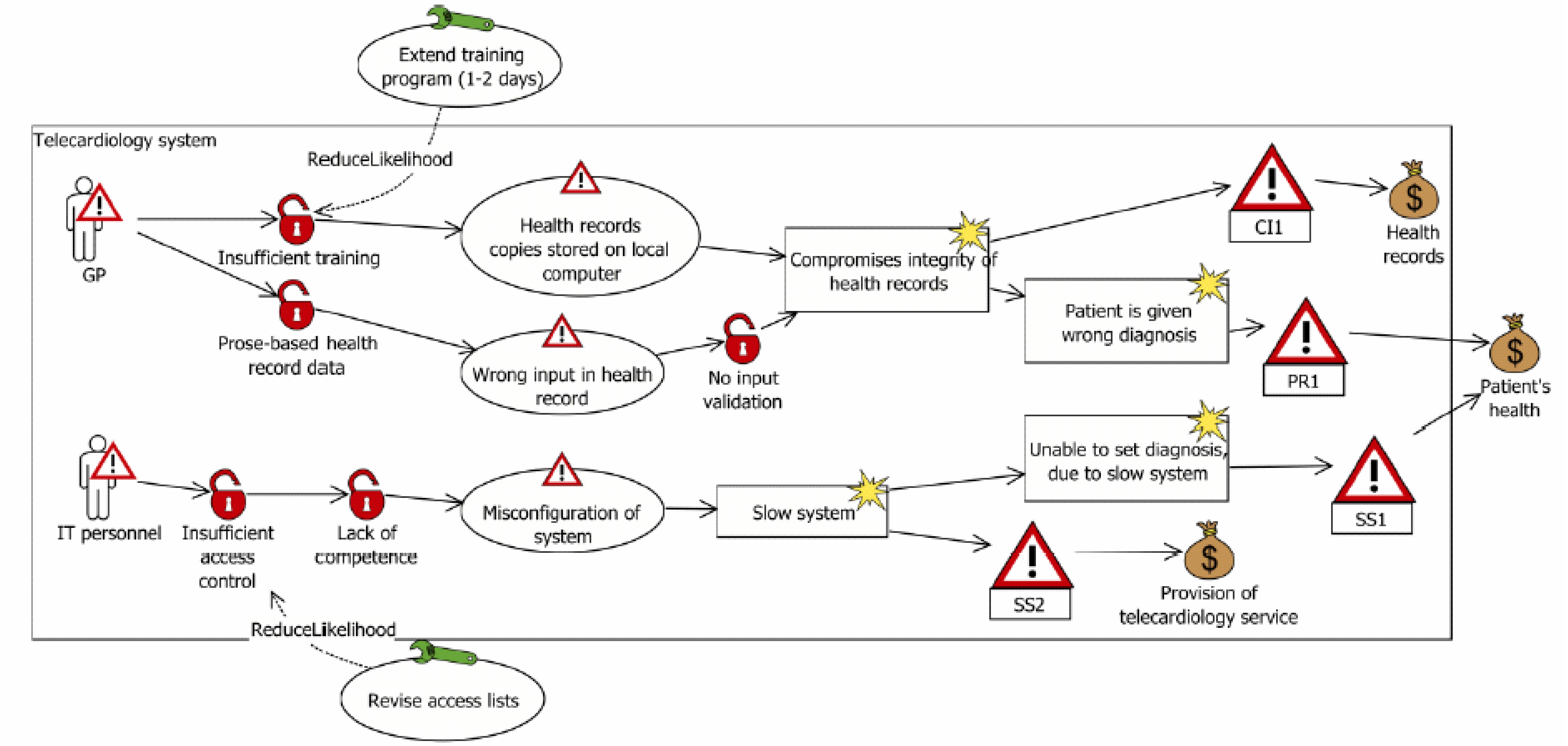
People that should participate

- Security analysis leader (required)
- Security analysis secretary (required)
- Representatives of the client:
  - Decision makers (required)
  - Technical expertise (required)
  - Users (required)

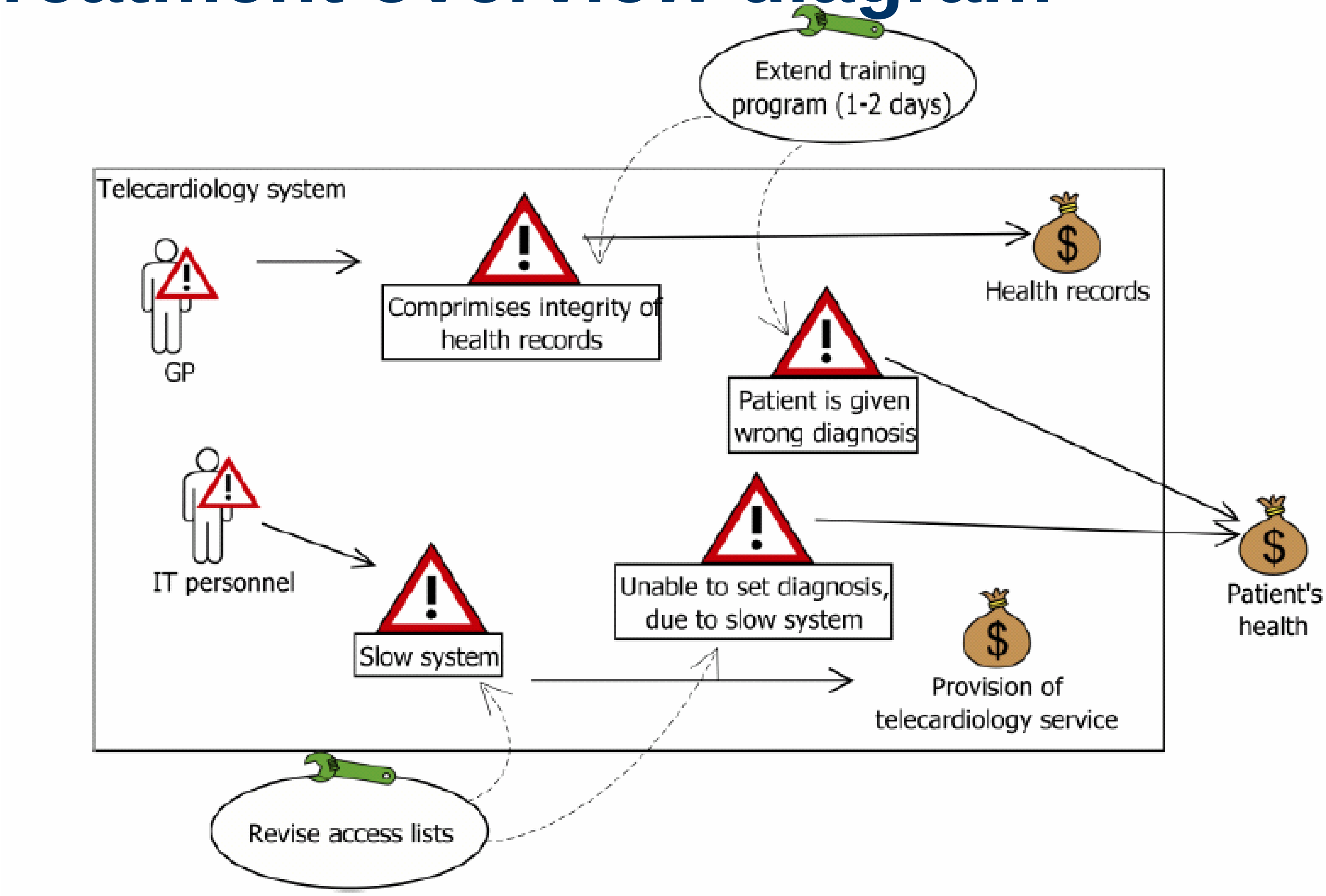
Modelling guideline

- Treatment diagrams:
  - Use the threat diagrams as a basis and annotate all arrows from unwanted incidents to assets with risk icons. Show only the unacceptable risks.
  - Annotate the diagram with treatments, pointing to where they will be applied.
- Treatment overview diagrams:
  - Use the risk diagrams as a basis, remove the acceptable risks.
  - Add treatments according to the treatment diagram(s).

Treatment diagram


Extend training program (1-2 days)
ReduceLikelihood
Telecardiology system
GP
Insufficient training
Prose-based health record data
Health records copies stored on local computer
Wrong input in health record
No input validation
Compromises integrity of health records
Patient is given wrong diagnosis
CI1
PR1
Health records
Patient's health
IT personnel
Insufficient access control
Lack of competence
Misconfiguration of system
Slow system
Unable to set diagnosis, due to slow system
SS1
SS2
Provision of telecardiology service
ReduceLikelihood
Revise access lists

Treatment overview diagram


Extend training program (1-2 days)
Telecardiology system
GP
Comprimises integrity of health records
Health records
Patient is given wrong diagnosis
IT personnel
Slow system
Unable to set diagnosis, due to slow system
Patient's health
Provision of telecardiology service
Revise access lists