

***Solution proposal
Oblig-III 2025***

KETIL STØLEN

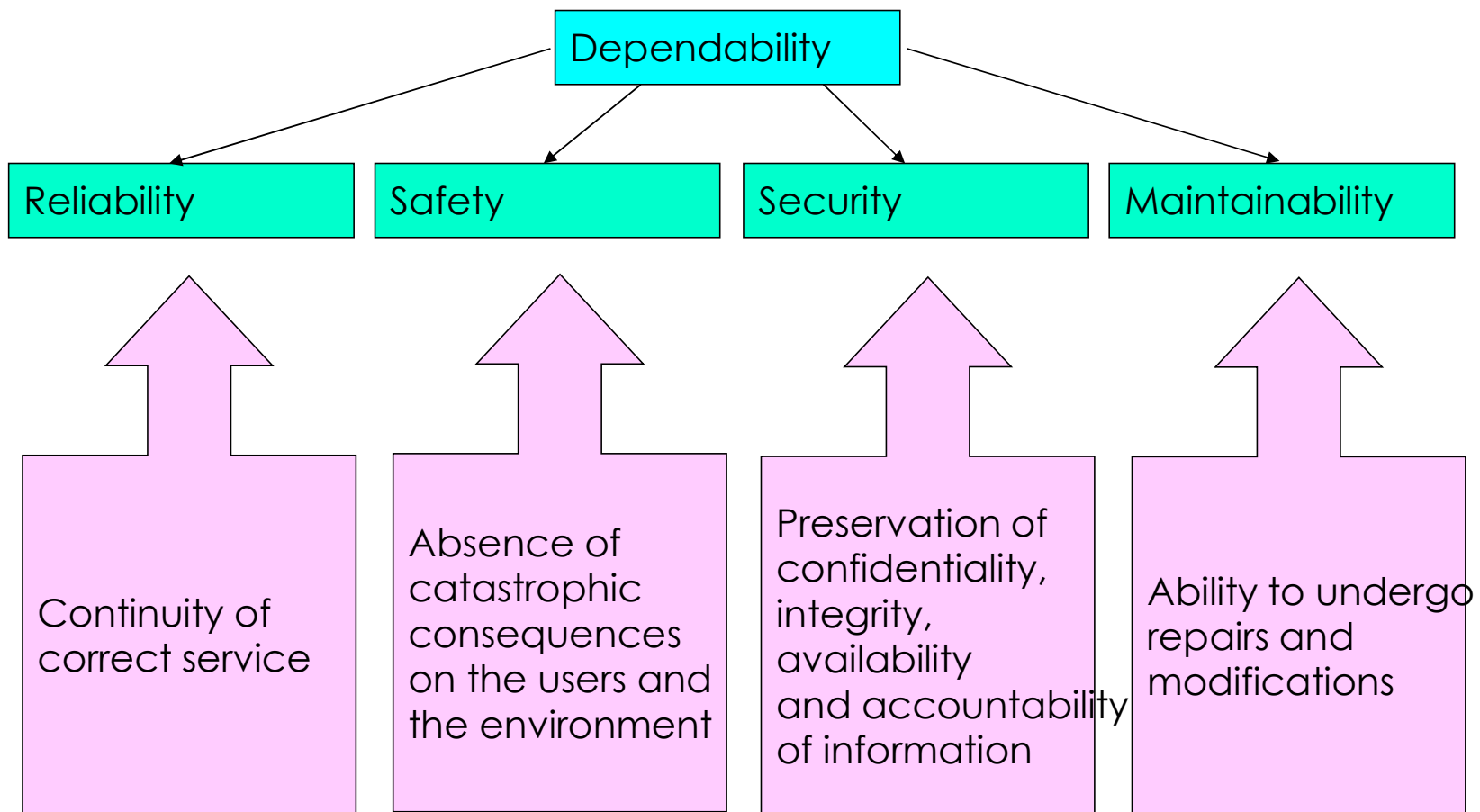
Question I

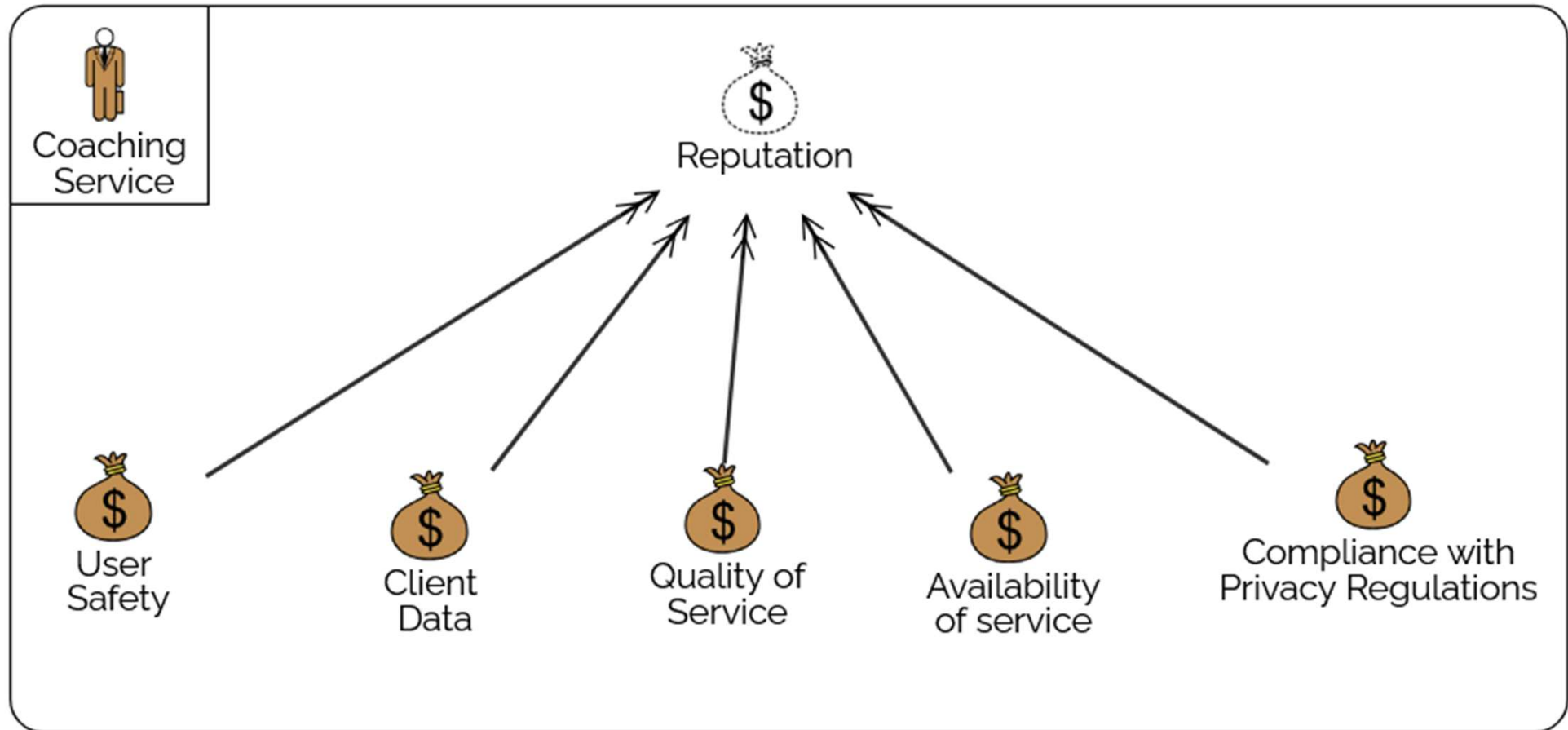
- There should be at least one indirect asset. One of the indirect assets should be reputation. Identify at least five direct assets of relevance for the party with respect to the indirect assets. Two of these five direct assets should be compliance with privacy regulations and user safety.
- Make a CORAS asset diagram that correctly relates them.

How we defined privacy (see first group)

- Privacy: the state of being free from intrusion or disturbance in one's private life or affairs

How we define safety (see first group)





Question II

- Make a good quantitative scale for measuring harm (consequence) to the asset compliance with privacy regulations. It should have at least 5 values.

Value	Average fine in 1000 Euro
Catastrophic	$[1000, \infty>$
Considerable	$[100, 1000>$
Significant	$[10, 100>$
Moderate	$[1, 10>$
Minor	$[0, 1>$

Question III

Make a good qualitative scale for measuring harm (consequence) to the asset user safety. It should have at least 5 values.

Value	Description
Catastrophic	Hospitalizing due to injury
Considerable	Sick leave due to injury
Significant	Physiotherapeutic treatment due to injury but no sick leave
Moderate	Training break of a couple of days
Minor	Some pain or stiffness, but able to continue training

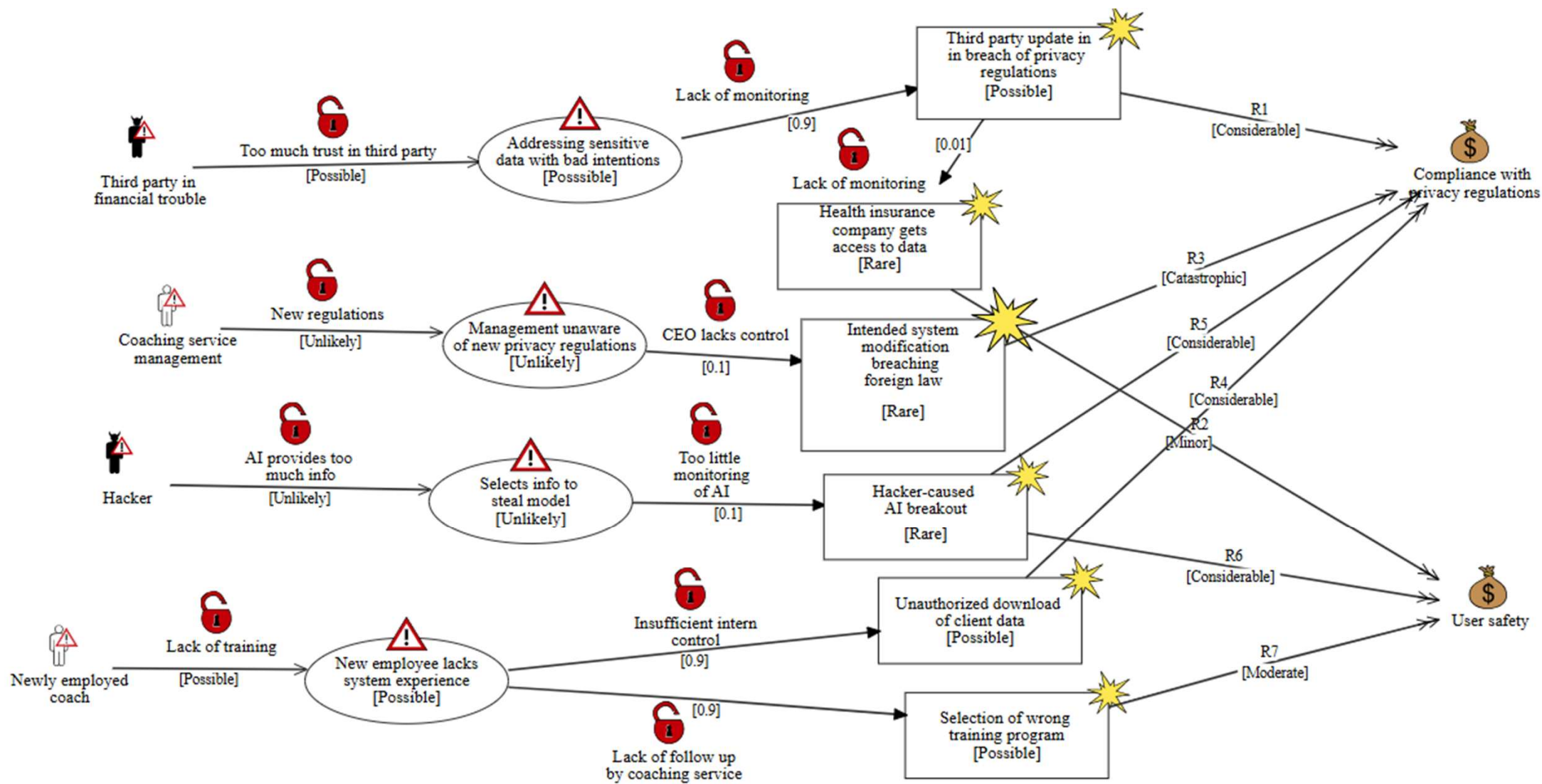
Question IV

Make a good quantitative interval scale for measuring likelihood using frequencies.

Frequency value	Intervals of average frequency per year
Common	$<12:1y, \infty:1y]$
Likely	$<1:1y, 12:1y]$
Possible	$<0.1:1y, 1:1y]$
Unlikely	$<0.01:1y, 0.1:1y]$
Rare	$[0:1y, 0.01:1y]$

Question V

Make relevant threat diagrams with respect to the two direct assets compliance with privacy regulations and user safety. The diagrams should all together capture at least seven risks. The diagrams should be annotated with consequences and likelihoods in such a way that they are consistent. Every initiate relation, unwanted incident and threat scenario should be assigned a frequency using the scale defined above. Every leads-to relation should be assigned a conditional probability different from 1. Moreover, all initiate, and leads-to relations should have at least one vulnerability associated with them (i.e. represented in the diagram).



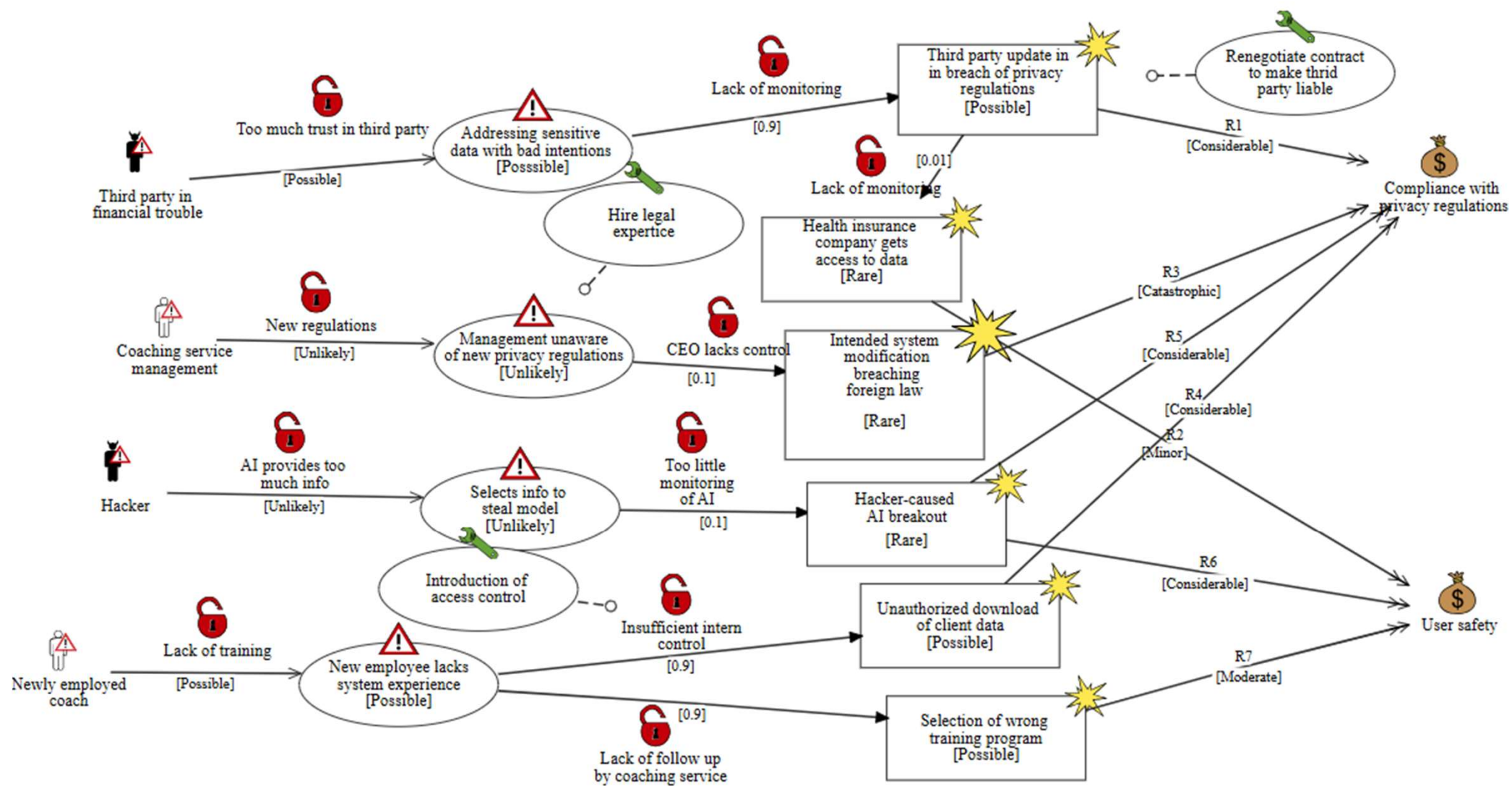
Question VI

Present the identified risks in a risk-matrix.

	Minor	Moderate	Significant	Considerable	Catastrophic
Common					
Likely					
Possible		R7		R1,R4	
Unlikely					
Rare	R2			R5, R6	R3

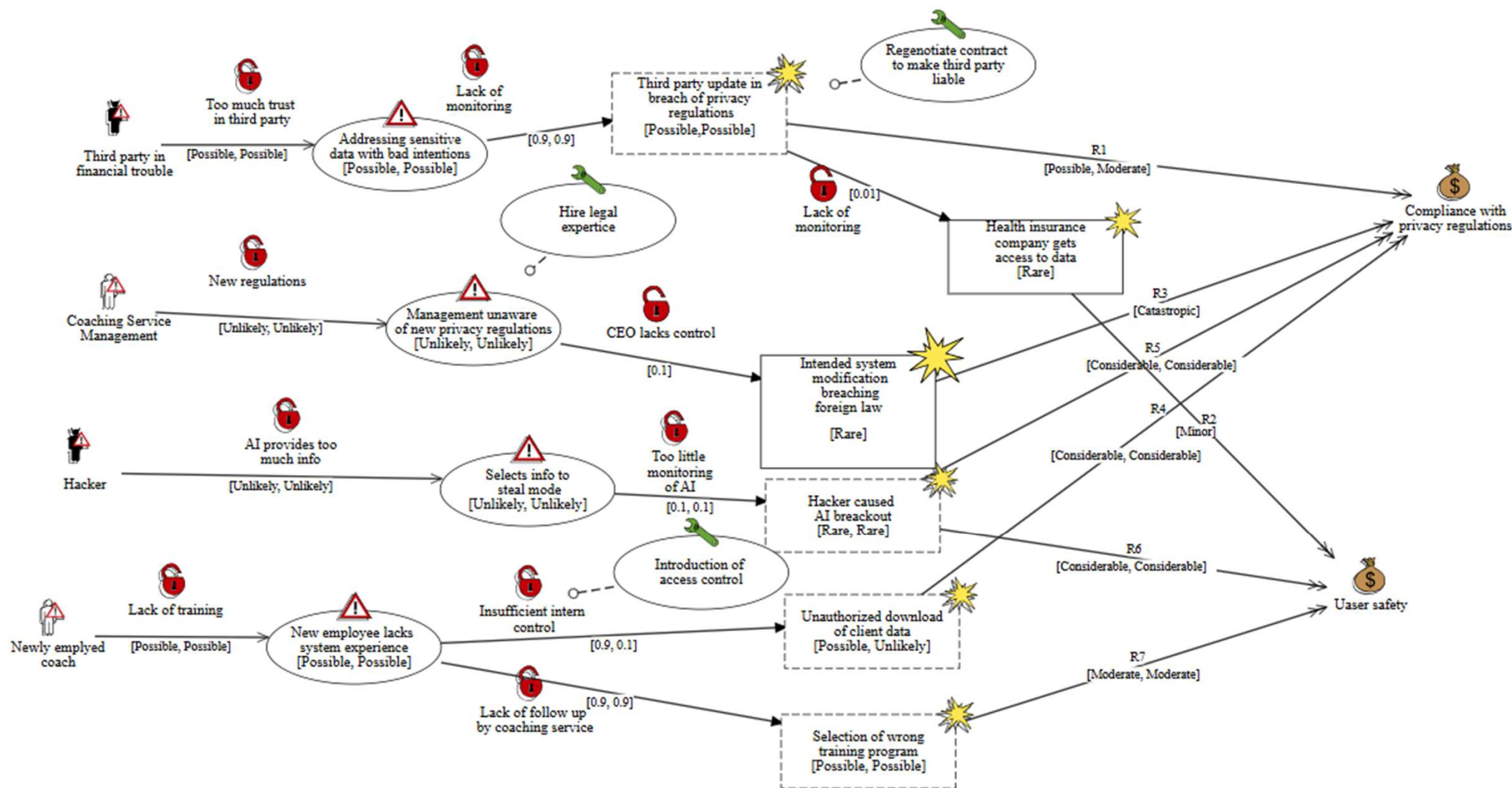
Question VII

Make a treatment diagram by annotating the threat diagrams from Question V with relevant treatments.



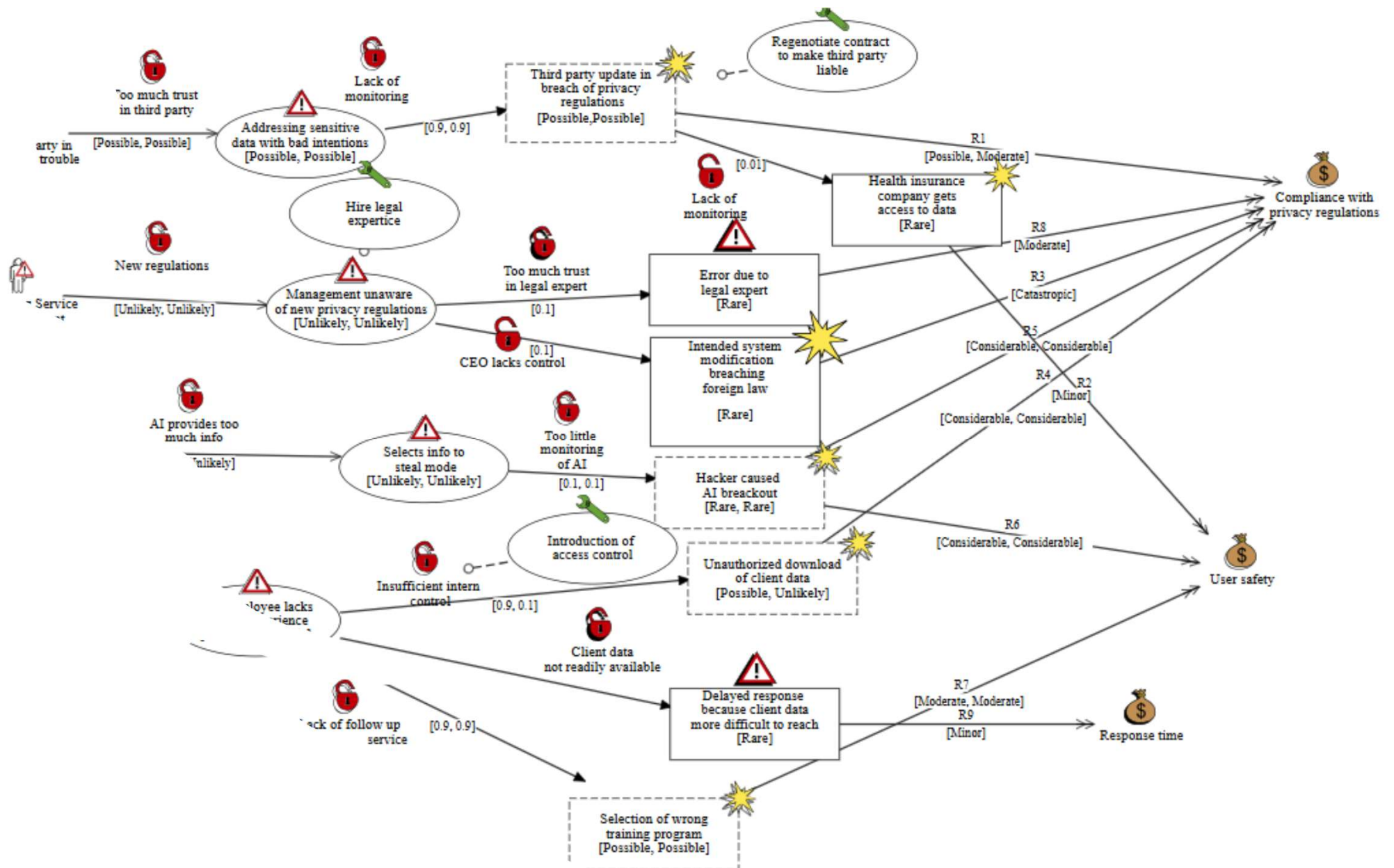
Question VIII

Assume that treatments are required for at least the three most important risks. Use the CORAS before-after style to illustrate the effect of these treatments on the already identified risks. The threat diagrams you have already drawn (Question V) correspond to the before situation. You are to "translate" these threat diagrams into threat diagrams expressed in the so-called before-after style reflecting the situation both before and after the implementation of the treatments.



Question IX

Any risk treatment will introduce some new risks (possibly with respect to some new assets). Update the threat diagrams from Question VIII to capture at least two new risks.



Question X

Present the risk matrix as it looks after the risk treatment (also considering the results from Question IX)

	Minor	Moderate	Significant	Considerable	Catastrophic
Common					
Likely					
Possible		R7, <u>R1</u> , <u>R7</u>		R1,R4	
Unlikely				<u>R4</u>	
Rare	R2, <u>R9</u>	<u>R8</u>		R5, R6, <u>R5</u> , <u>R6</u>	R3

The risk values changed due to treatment and the new risks are in bold and underlined

Note that the risks R2 and R3 only exist in the before state