

***Solution proposal
Oblig-III 2024***

KETIL STØLEN

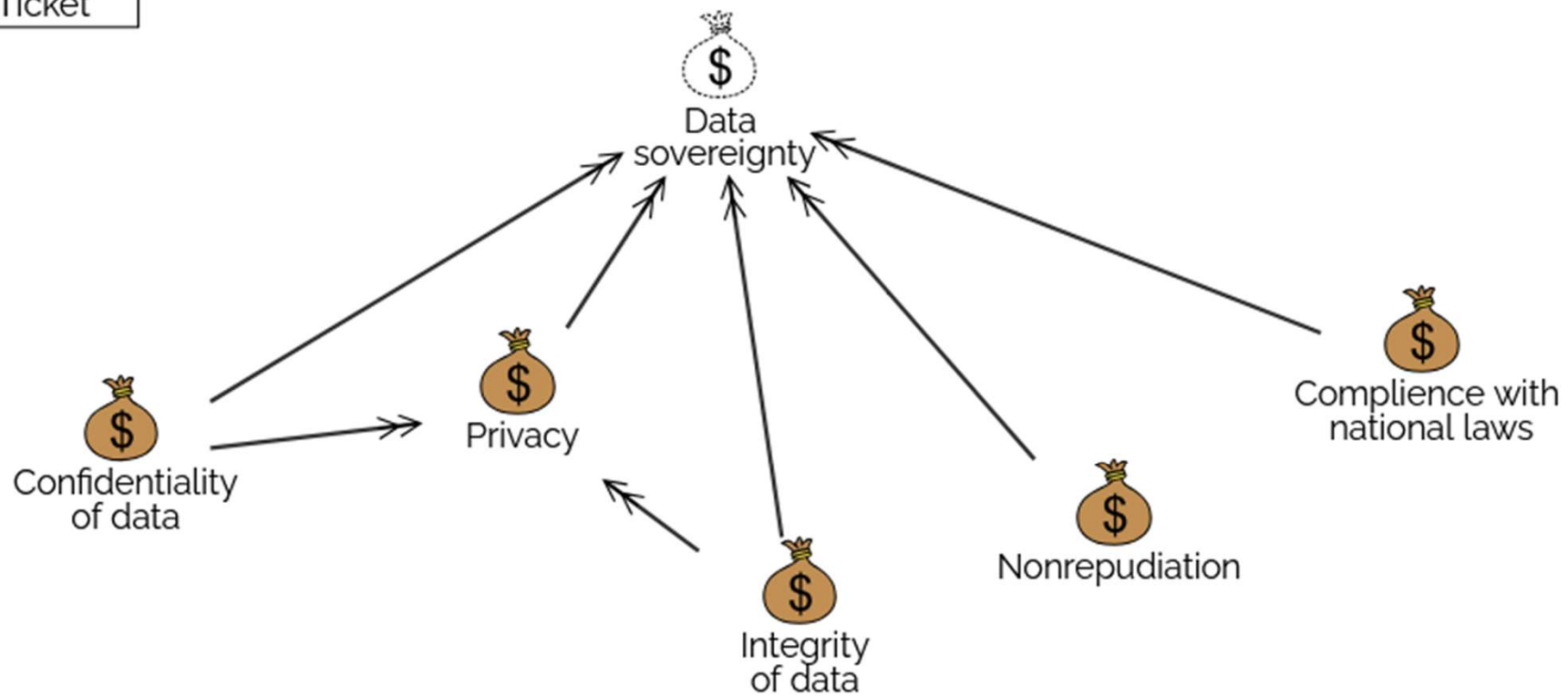
Question 1

There should be at least one indirect asset. One of the indirect assets should be data sovereignty. Data sovereignty is the idea that data are subject to the laws and governance structures of the nation where they are collected.

- 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 national laws and integrity of data.
- Make a CORAS asset diagram that correctly relates them.



Event
Ticket



Question 2

Make a good qualitative scale for measuring harm (consequence) to the asset compliance with national laws. It should have at least 5 values.

Value	Definition
Catastrophic	The company goes bankrupt
Considerable	Major fine reducing overall annual profit significantly
Significant	Fine and bad publicity
Moderate	No fine, but bad publicity
Minor	No fine and no publicity, but will probably be monitored carefully in the future by the authorities

Question 3

Make a good quantitative scale for measuring harm (consequence) to the asset integrity of data. It should have at least 5 values.

Value	Percentage of data modified in average
Catastrophic	<80,100]
Considerable	<60,80]
Significant	<40,60]
Moderate	<20,40]
Minor	[0,20]

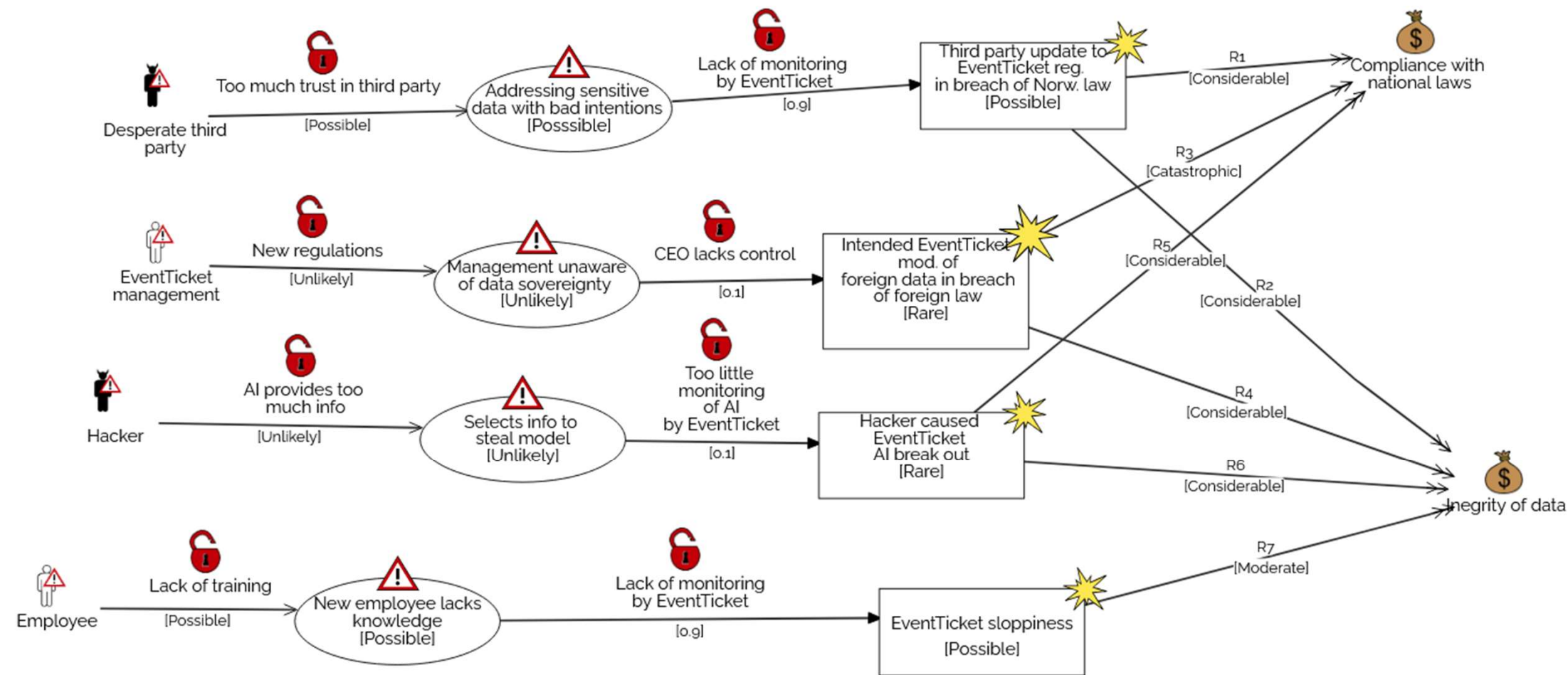
Question IV

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

Frequency value	Intervals of average frequency
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 national laws and integrity of data. 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).



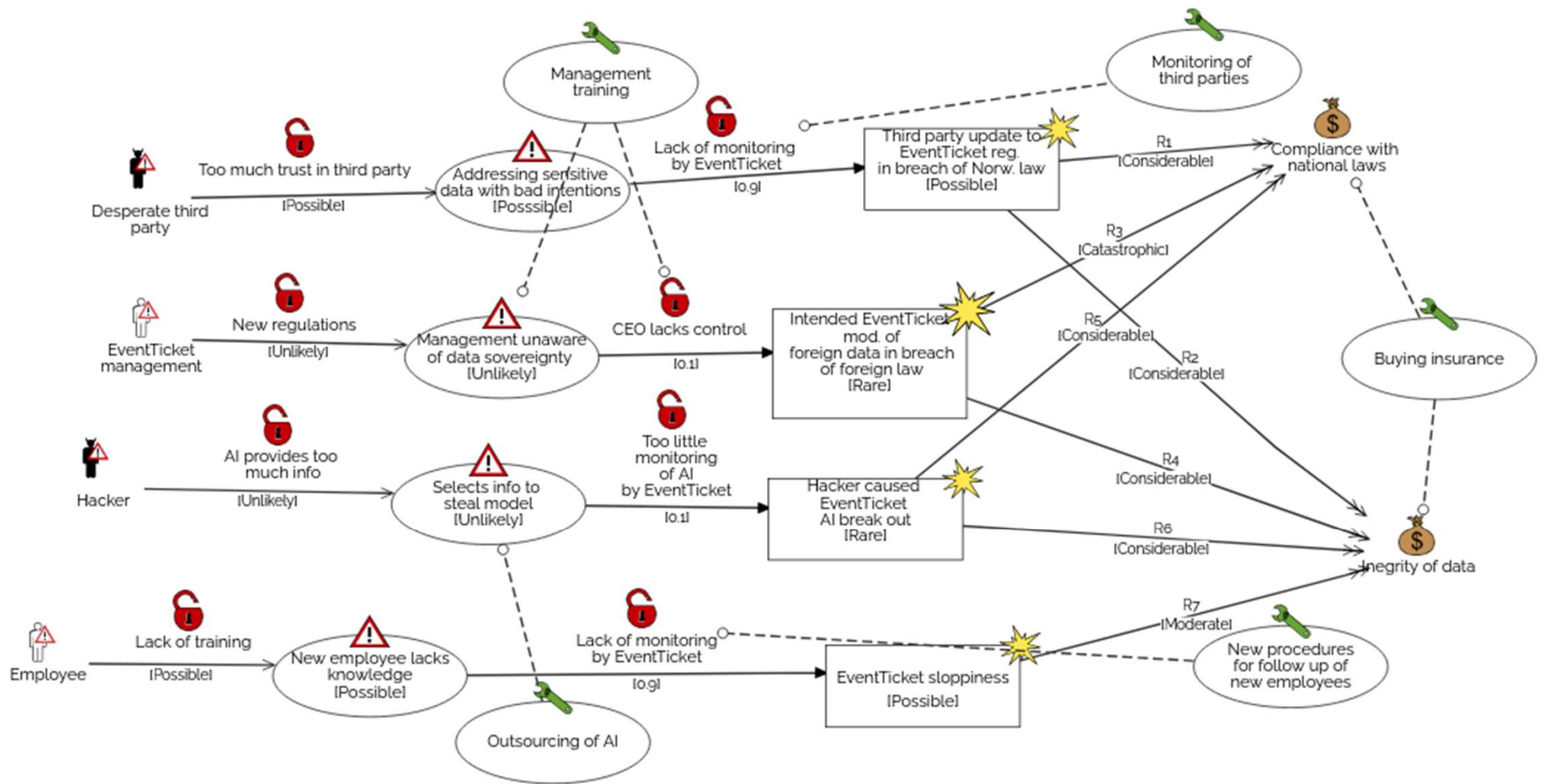
Question VI

Present the identified risks in a risk-matrix.

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

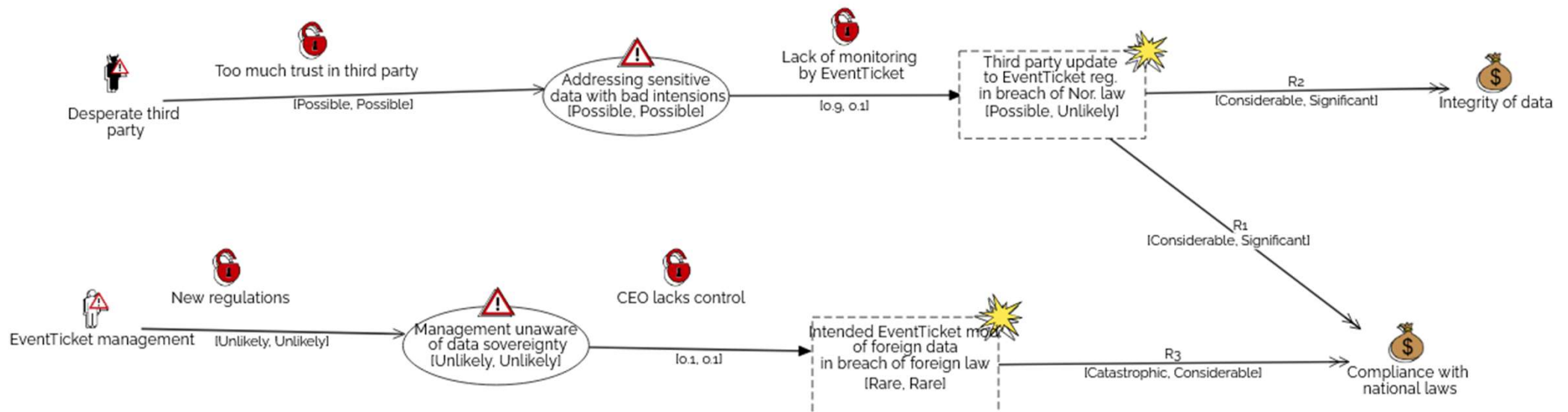
Question VII

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



Question VIII

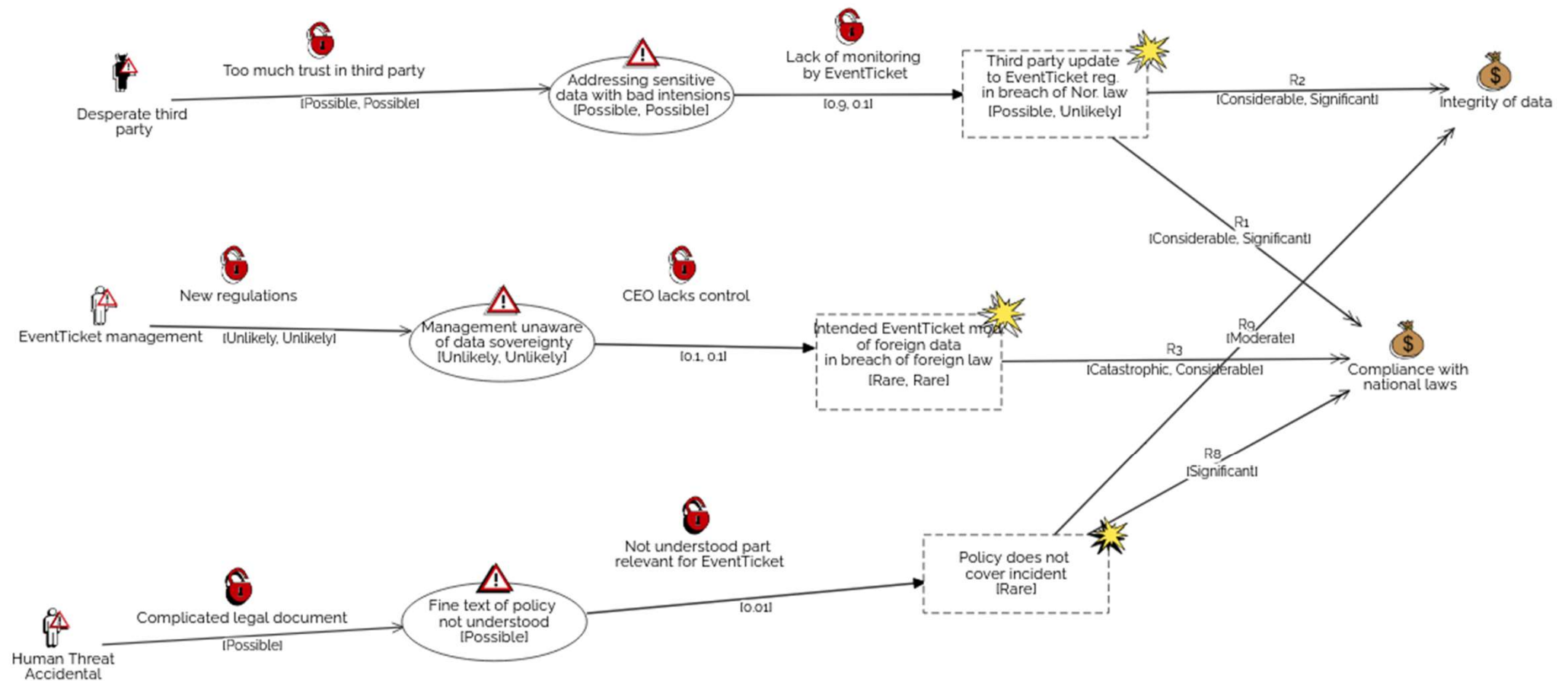
Assume that treatments are required for at least the three most important risks. Use the CORAS before-after style to illustrate the effect of these treatments on the already identified risks. The threat diagrams you have already drawn (Question V) correspond to the before situation. You are to "translate"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



Before-after threat diagram after buying insurance and improving the monitoring of third parties. Everything else in the original threat diagram is unchanged in the after state and therefore left out.

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		R1, R2	
Unlikely		<u>R9</u>	<u>R1, R2</u>		
Rare			<u>R8</u>	<u>R3</u> , R4, R5, R6	R3

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