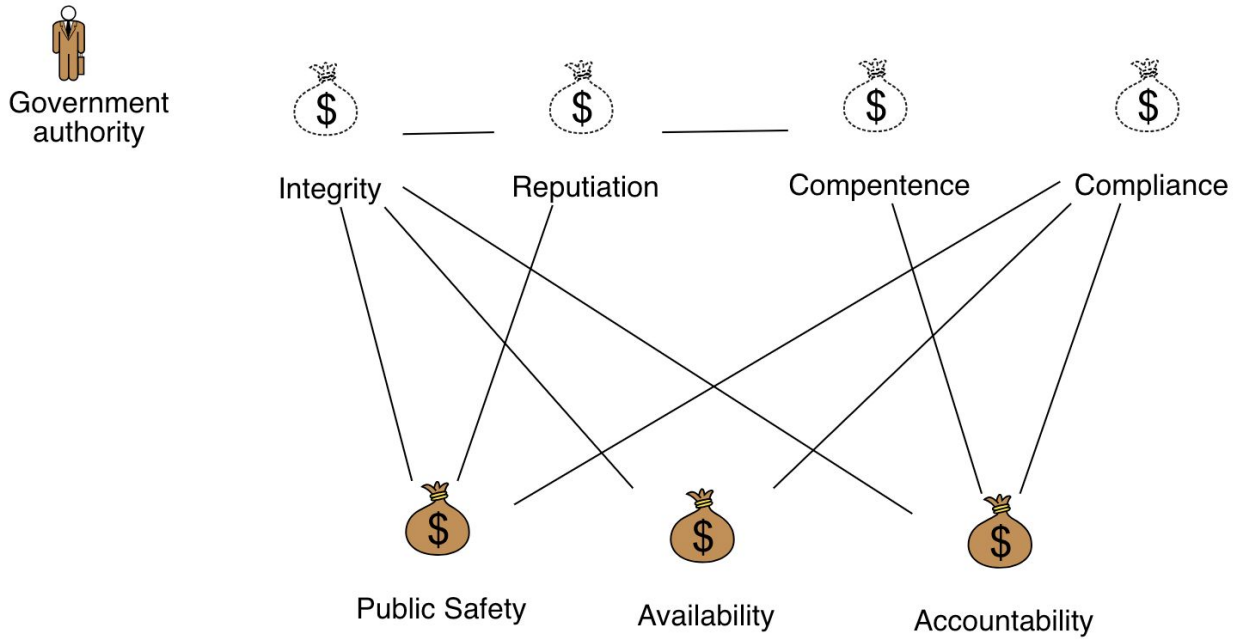
IN5130 - Oblig III

Security Risk Assessment of product monitoring during shipping

Birashanthan Tharmakulasingam and Tanusan Rajmohan

University of Oslo

Question I



Question II

Make a good ordinal scale for measuring harm (consequence) to the asset "**Public safety**".

Public Safety

Consequence	Description
4	Chemicals being leaked, and contaminating water reservoirs
3	Wrong chemicals distributed
2	Chemicals do not hold standard
1	Breaking traffic rules during shipment
0	No hazardous effect on shipment

Question III

Quantitative scale for measuring harm (consequence) to the asset "**Accountability**"

Consequence	Description
Catastrophic	[70%, 100%] of shipment does not reach customer
Major	[40%, 70%〉of shipment does not reach customer
Moderate	[1%, 10%〉 of shipment does not reach customer
Minor	[0.1%, 1%〉 of shipment does not reach customer
Insignificant	[0%, 0.1%〉 of shipment does not reach customer

Question IV

Consequence scales for the other direct assets you have identified, as well as a quantitative scale for likelihood based on frequencies.

Availability

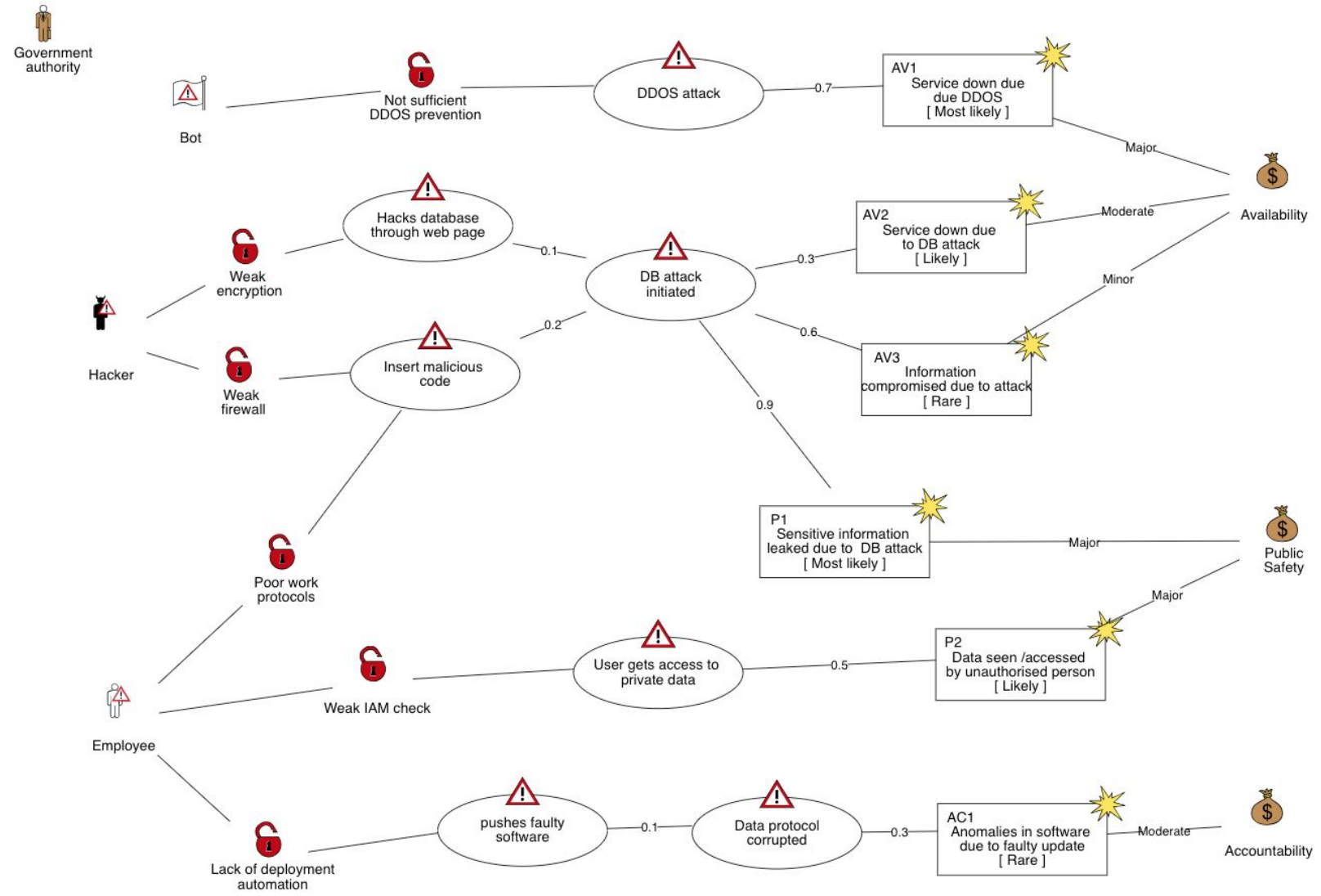
Consequence	Description
Catastrophic	[70%, 100%] of distributors cannot issue supplies
Major	[40%, 70%〉of distributors cannot issue supplies
Moderate	[1%, 10%〉of distributors cannot issue supplies
Minor	[0.1%, 1%〉of distributors cannot issue supplies
Insignificant	[0%, 0.1%〉of distributors cannot issue supplies

Database

Consequence	Description
Catastrophic	[70%, 100%] of data becomes compromised
Major	[40%, 70%〉of data becomes compromised
Moderate	[1%, 10%〉 of data becomes compromised
Minor	[0.1%, 1%〉 of data becomes compromised
Insignificant	[0%, 0.1%〉 of data becomes compromised

Question V

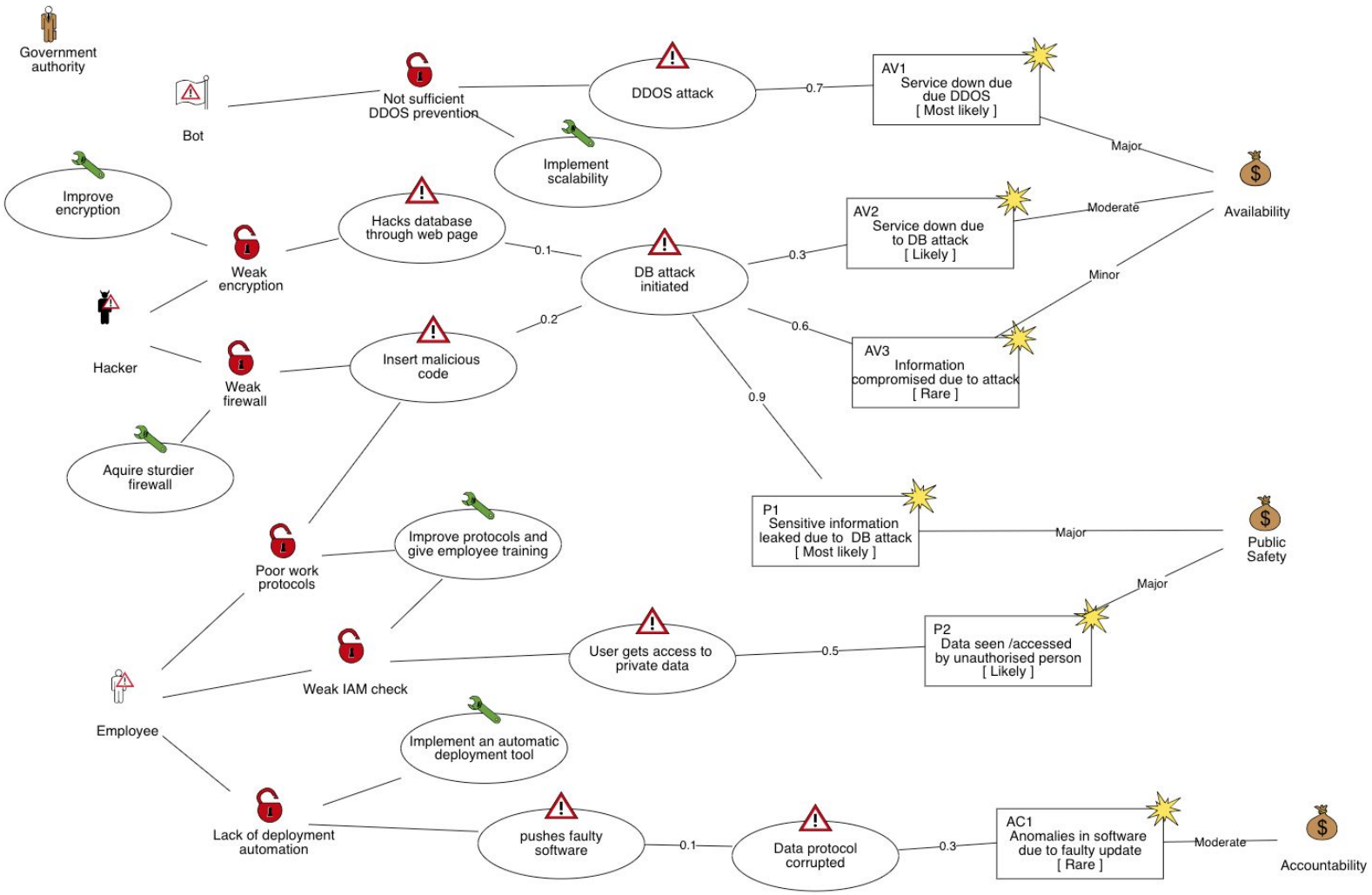
Make a threat diagram with respect to the direct assets. The diagrams should all together capture at least seven risks.



Question VI

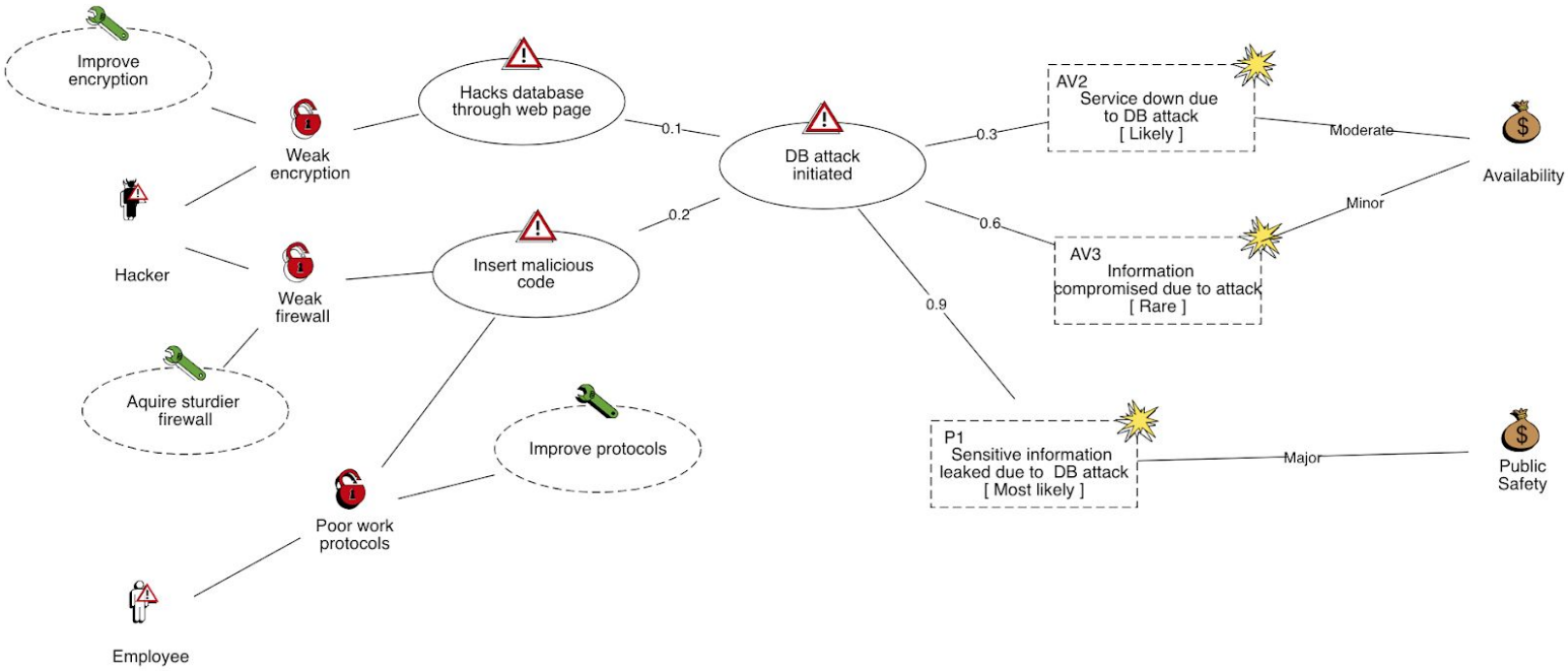
	Insignificant	Minor	Moderate	Major	Catastrophic
Rare		AV3	AC1		
Unlikely					
Likely			AV2	P2	
Most likely				P1, AV1	
Certain					

Question VII



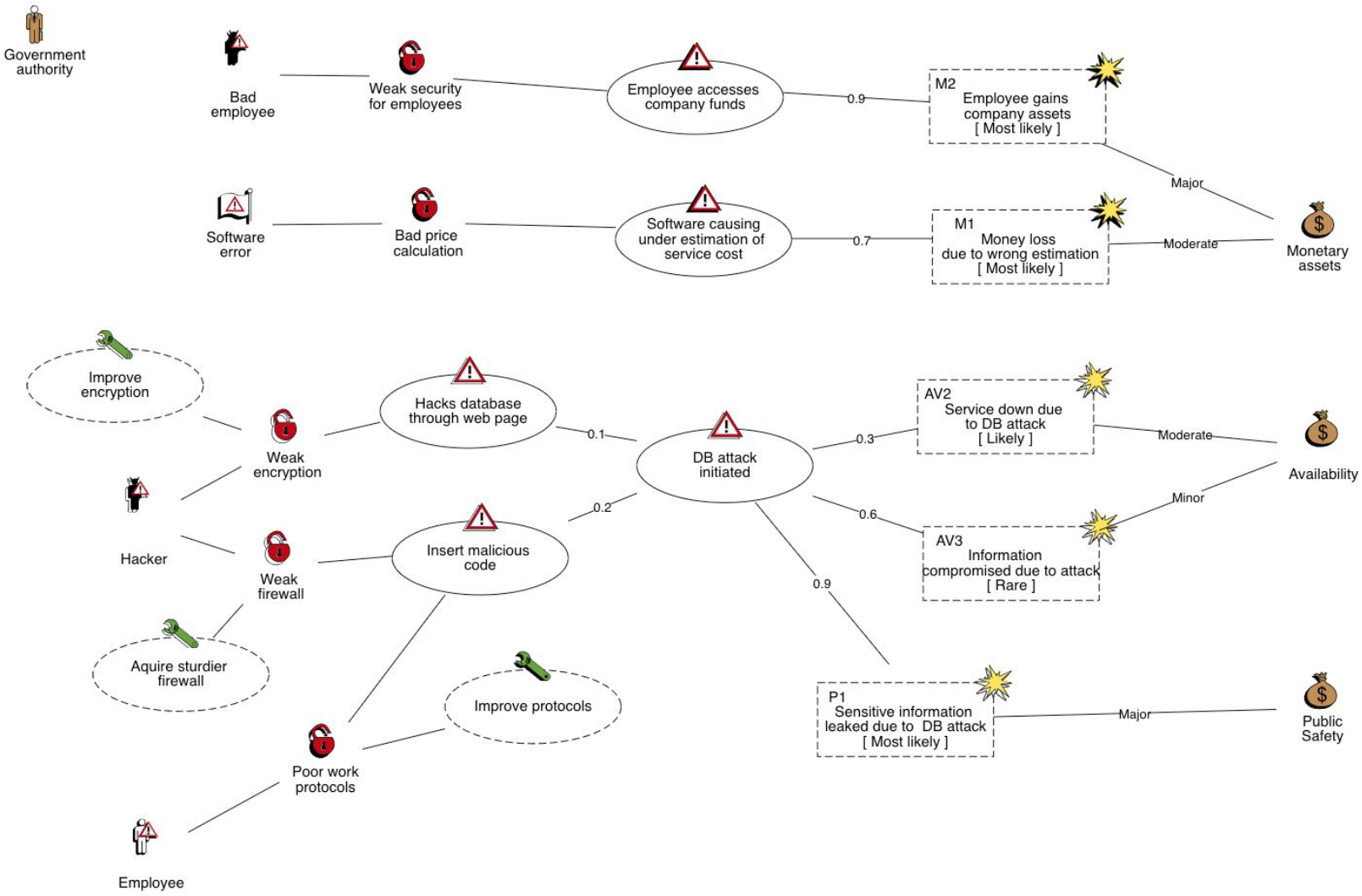
Some new risk might be introduced due to the introduction of the treatments which we have shown in question IX. For example, the DDOS measures might think that a regular employee is trying to do a DDOS attack, when in reality he/she is just trying to acquire a lot of data, thus sending a lot of request. Another thing might be that the automatic deployment tool might be bugged, and upload some code it is not supposed to do, or some employees might accidentally override the automatic deployment process. This will further be explored in next tasks.

Question VIII



We assumed in this task that we were supposed to remove the incidents and risks for the treatments we chose to fix. This is why the diagram is smaller, but we implemented before-after in a way that everything that was impacted by the change became “after” in the new diagram. While the unchanged parts will be placed as “before”.

Question IX



Here we chose to introduce two new risk which lead to a new asset, instead of making the risks mentioned in task VII,

Question X

	Insignificant	Minor	Moderate	Major	Catastrophic
Rare		AV3			
Unlikely					
Likely			AV2		
Most likely			M1	M2, P1	
Certain					

As you can see we ended up with less risks in the high risk portion of the matrix. This is because it was based on the new diagram where we removed the major risks and implemented new.