

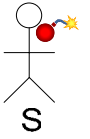
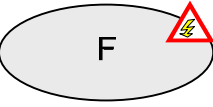

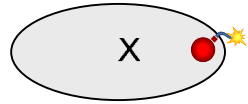

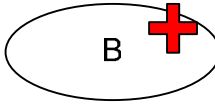
Modelling exercises

Introduction

This exercise is about the threat modelling using the CORAS language:

- This first section considers common modelling tasks during a risk analysis.
- The second section considers various ways of modelling the same situation and your task is to prioritize between them and choose the way you think is best!

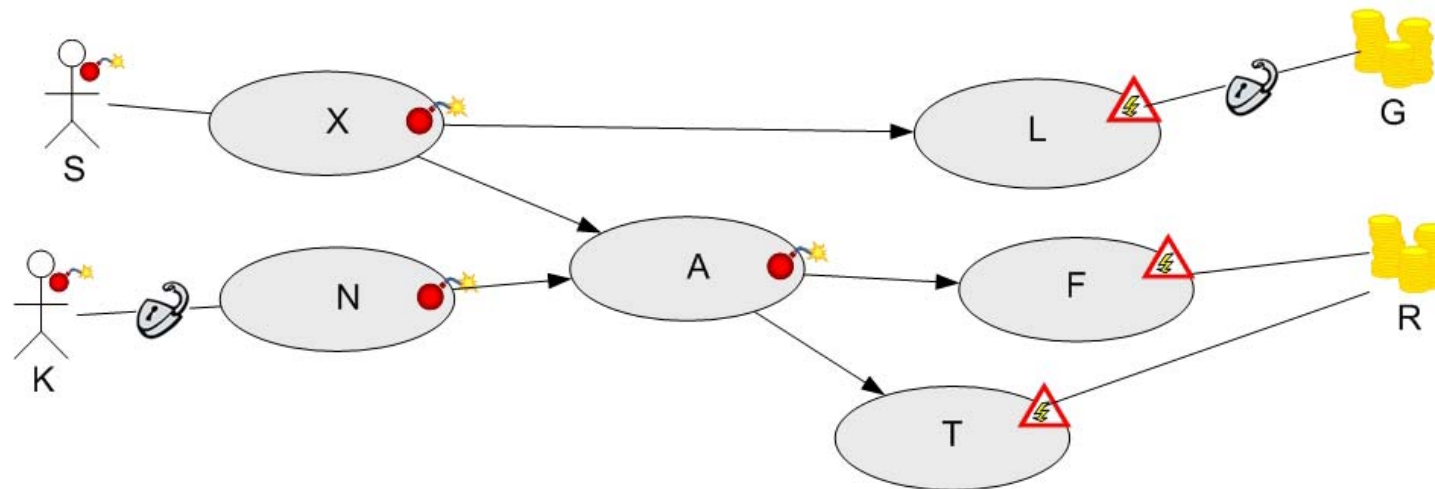
The symbols and definitions we use from the CORAS language is described in this table:

Symbols					
 S	Threat: someone/something that intentionally or non-intentionally can cause an event that may harm an asset.	 F	Incident scenario: sequence of events leading to an unwanted incident	 G	Asset: something of value which needs to be protected.
 X	Threat scenario: a sequence of events corresponding to a threat exploiting vulnerabilities.		Vulnerability: a weakness or a lack that a threat can exploit.	 B	Treatment scenario: a description of the actions made to reduce a risk.

Common modelling tasks

1)

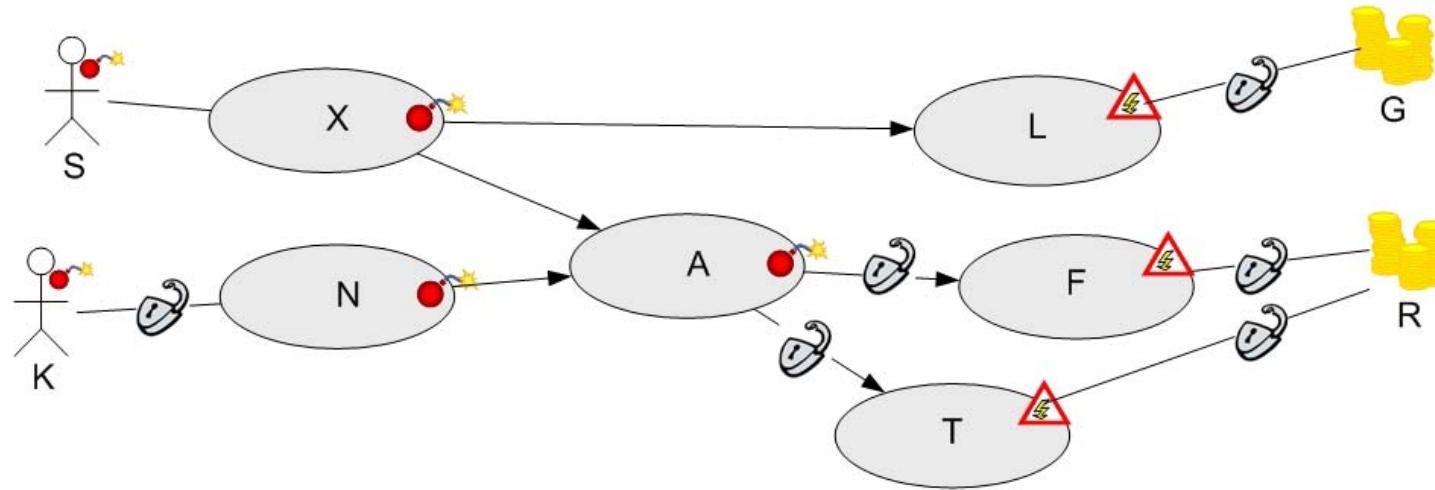
To harm asset R threat S must exploit at least one vulnerability, - give an example of where this vulnerability can be by marking with a cross in the diagram:



2)

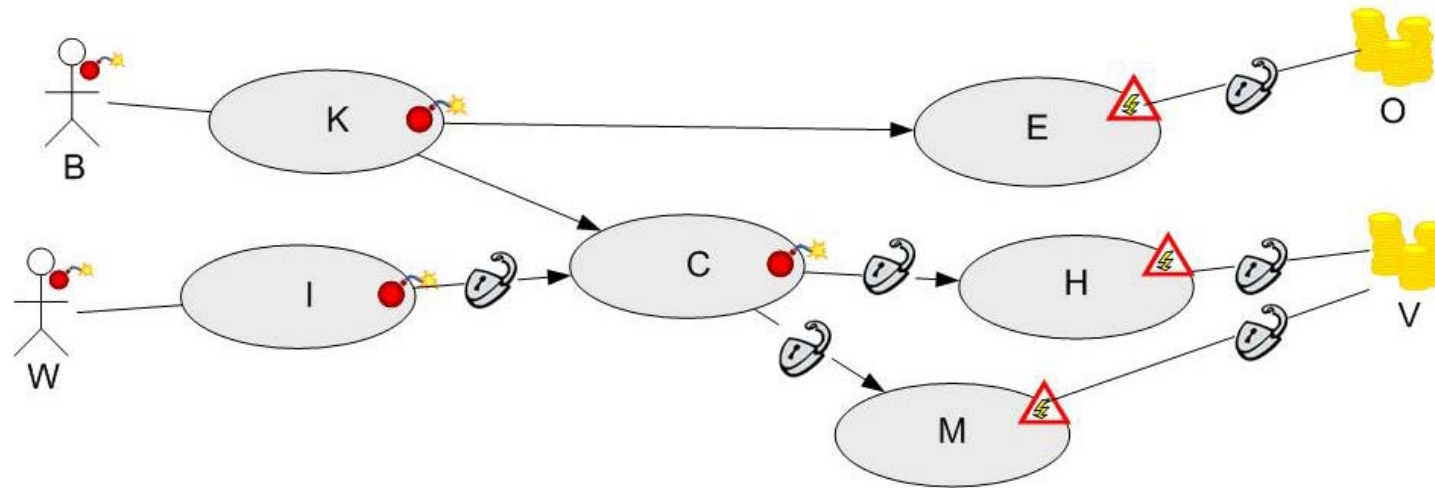
How many vulnerabilities can threat K exploit to harm asset R? (mark with an X for correct number):

1	2	3	4	5	6
---	---	---	---	---	---



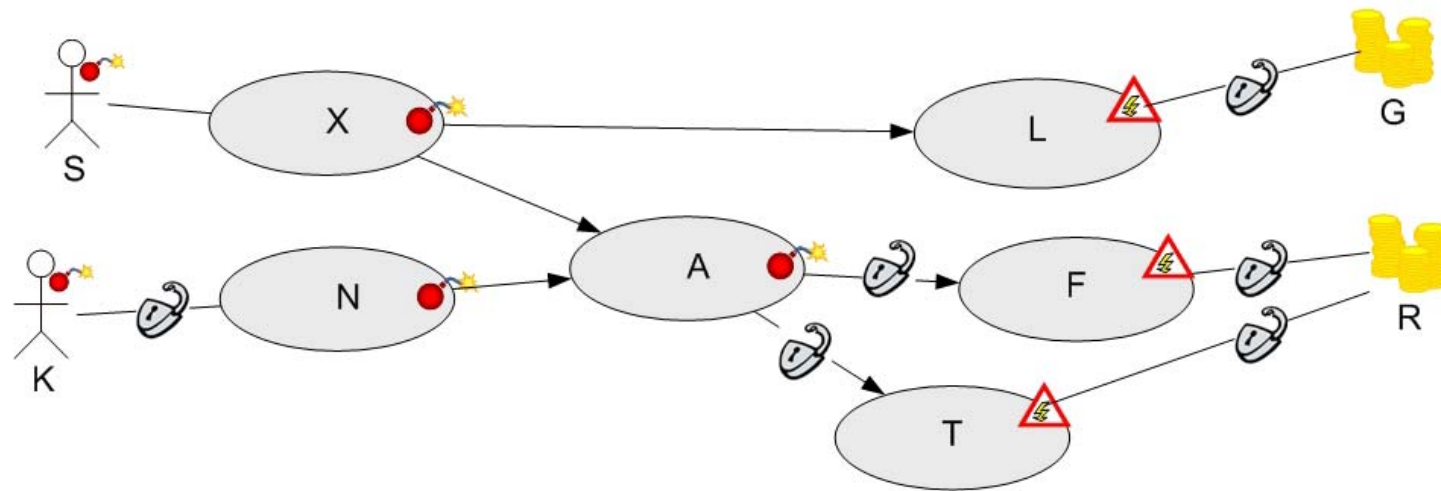
3)

Extend the diagram with a new incident scenario (U) for an unwanted originating from threat scenario I and harming asset V:



4)

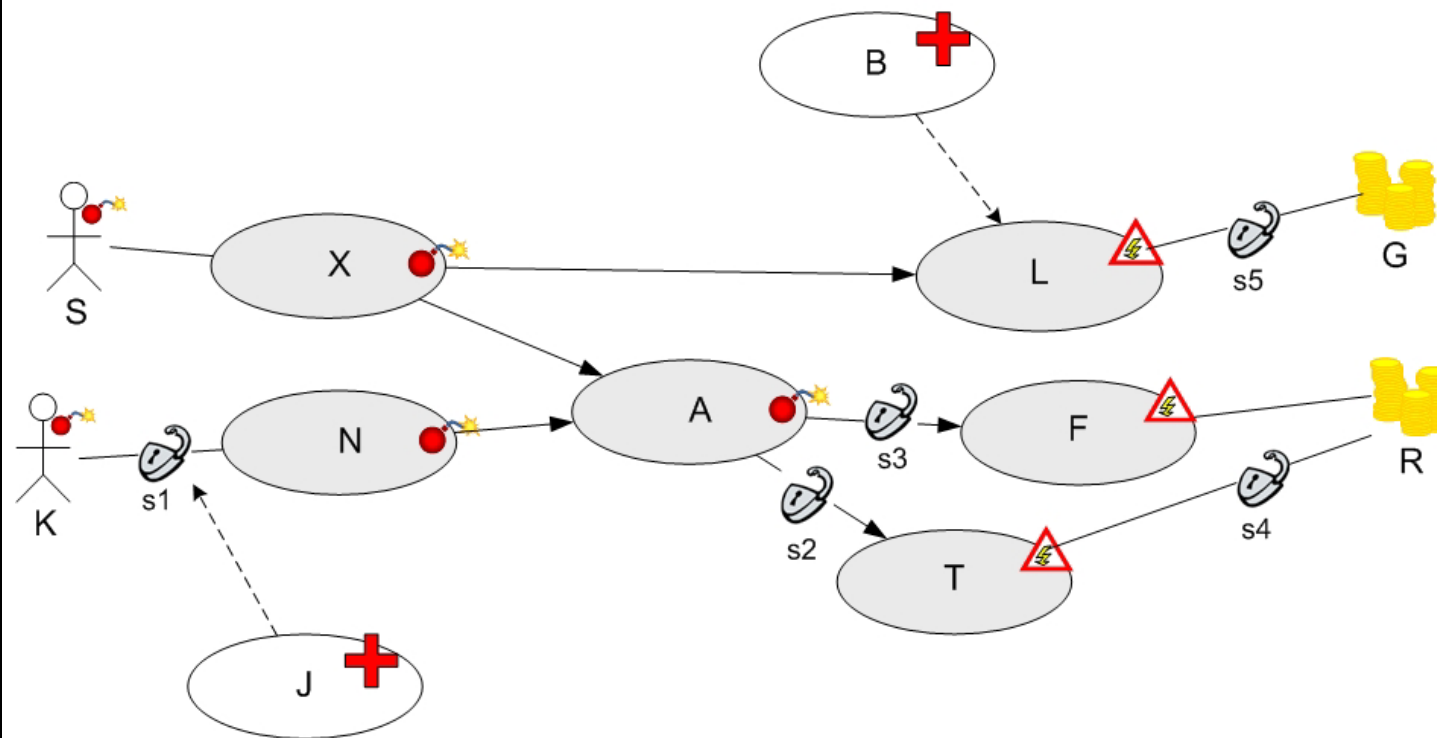
Add a new threat (P) that behaves identical to threat K:



5)

The diagram below is extended with treatments scenarios: treatment B is directed towards the unwanted incident of incident scenario L and treatment J is directed towards vulnerability s1. You should do the following:

- add a new treatment scenario (M) towards an unwanted incidents that has not been treated
- show that treatment J also can be used against s2



6)

Model the following scenario:

An employee in a large company infects unintentionally the company network with a worm which attacks the mail server and makes it impossible to receive or send email for a whole day. The worm first infects the employee's computer due to the company's insufficient antivirus solution.

- a) Model the asset which is harmed in this scenario as well as the threat, vulnerability, threat scenario(s), and incident scenario(s).
- b) When the worm is investigated further they see that it also attacks file storage servers that keep important company information, add this information to the model.

7)

Model the following scenario:

A phone exchange building (telefoncentral) is struck by lightning which causes a fire. The fire destroys vital phone equipment which means that nobody in the area is able to use their telephone. Model this scenario from the phone users' perspective, not the phone company.

- a) Model the threat(s), threat scenario(s), vulnerability (or vulnerabilities), incident scenario(s) and asset(s) in this situation
- b) In addition to the danger of lightning, there is also a pyromaniac (pyroman) in the area, -extend the model with this information
- c) If you were to see this from the phone company's point of view, how would you change the model?

Prioritizing different ways of modelling threat diagrams

Compare two and two diagrams and choose the one you prefer by marking with an "X" in the table below the weight symbol, like shown in this example:

Which diagram do you prefer, diagram 1 or diagram 2?

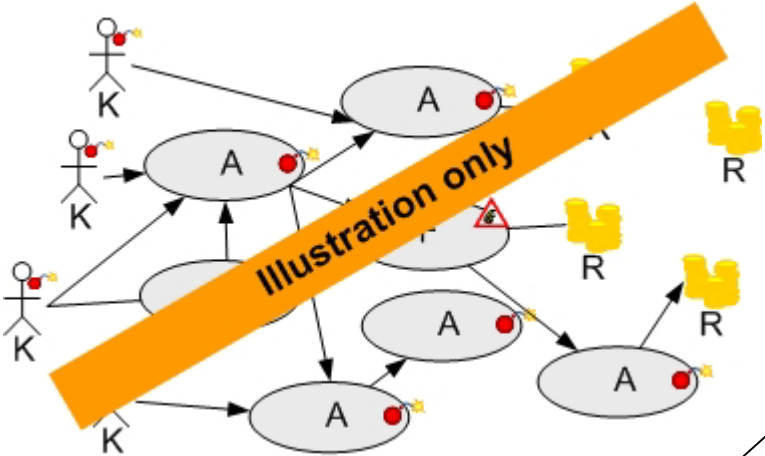



Diagram 1



	X						
--	---	--	--	--	--	--	--

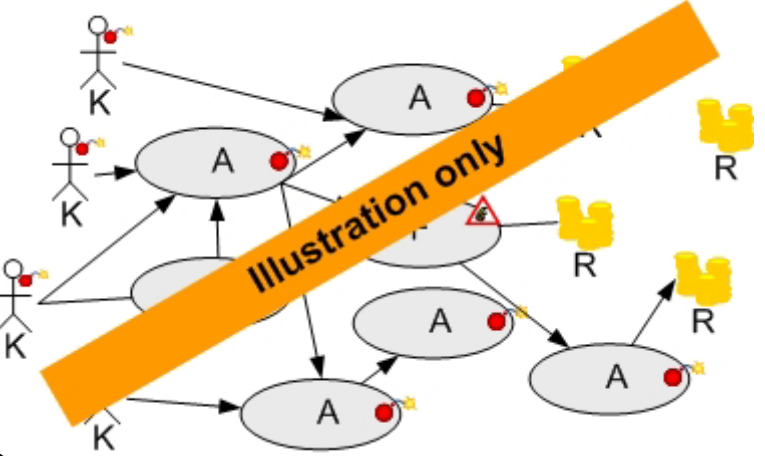


Diagram 2

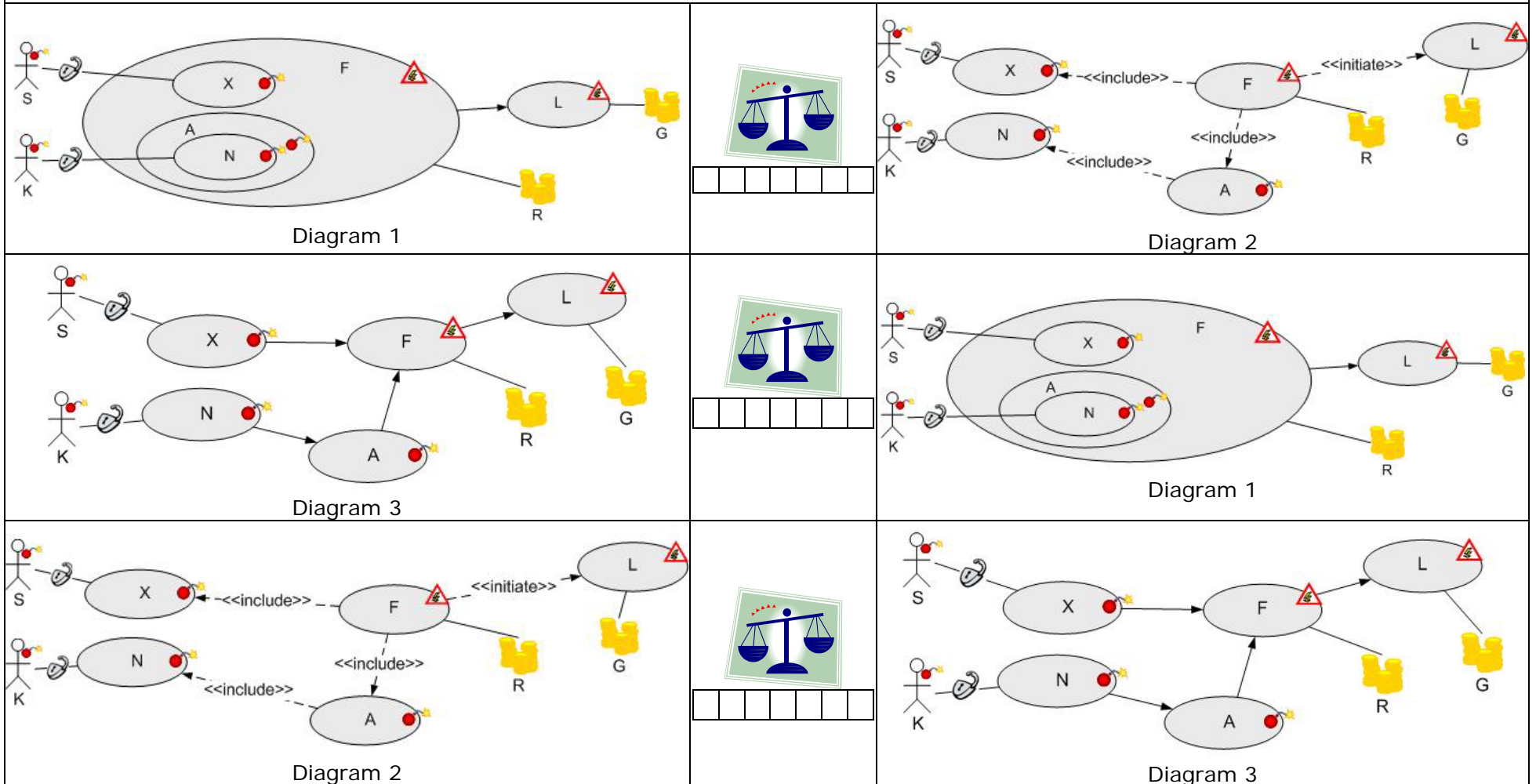
"I prefer diagram 1"

"I think they are equally good"

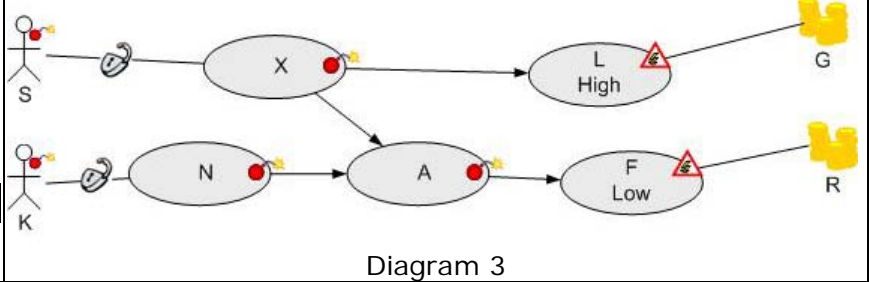
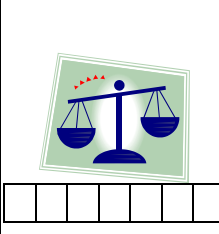
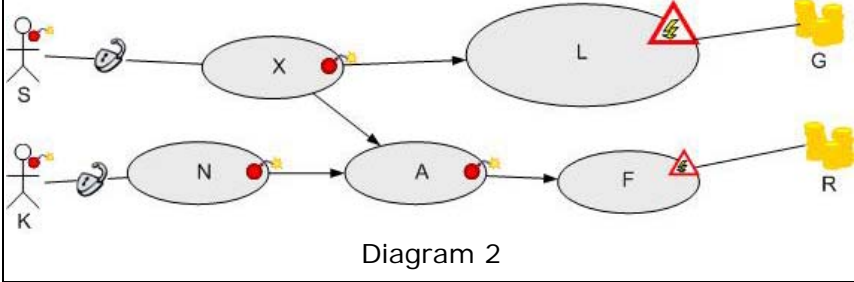
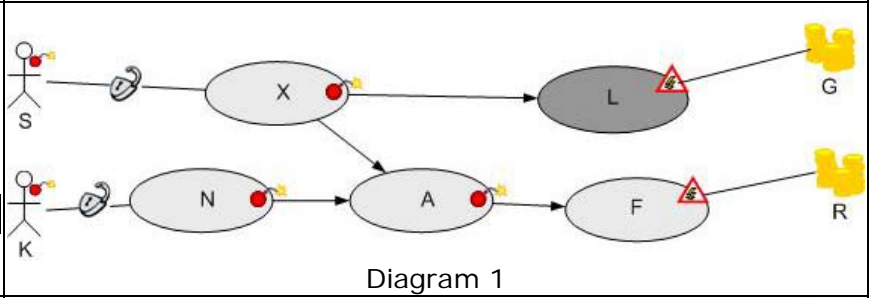
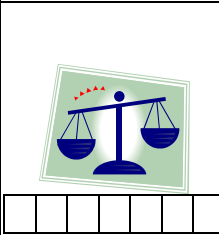
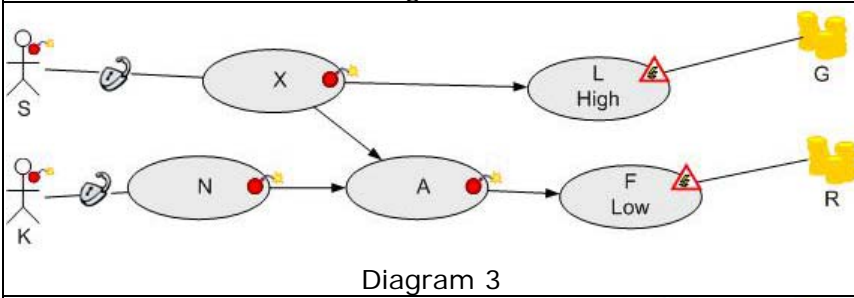
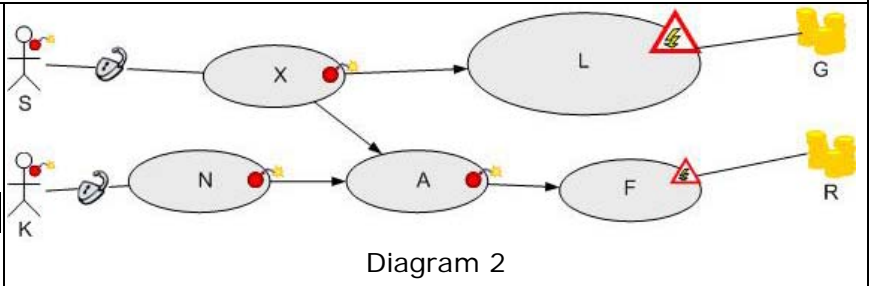
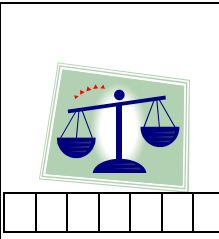
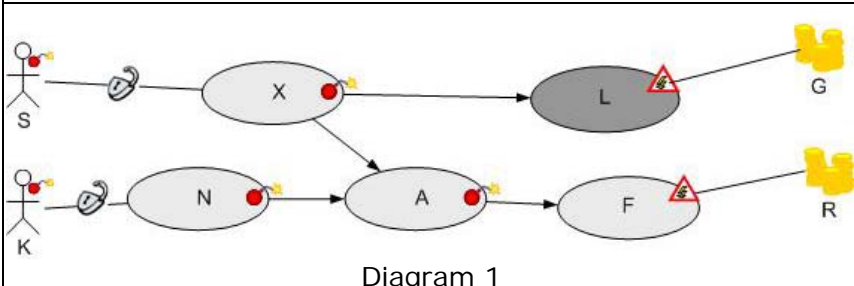
"I prefer diagram 2"

"Diagram 1 is better than diagram 2, but still not my favourite"

8) Which diagram shows best that threat scenario N can cause the unwanted incident of incident scenario L?



9) Which diagram shows best that the unwanted incident of incident scenario L is more serious than unwanted incident of F?



10) Which diagram shows best that it is more likely that T happens after A, than L or F?

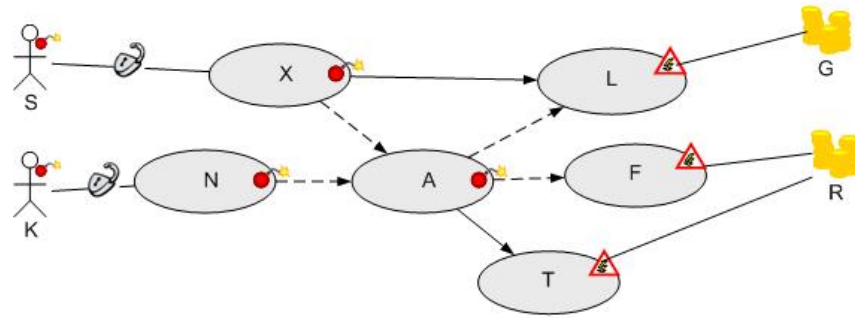


Diagram 1

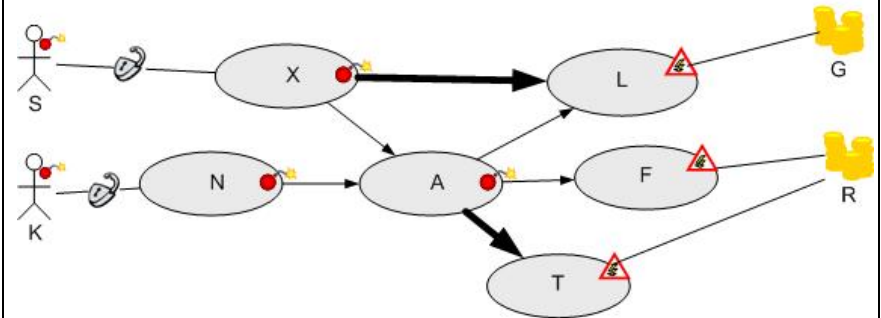
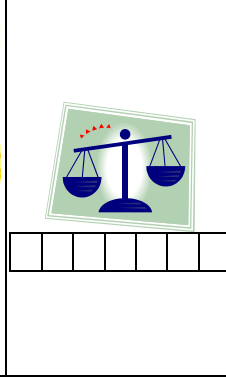


Diagram 2

11) Which diagram shows best that both X and N must happen before A can happen?

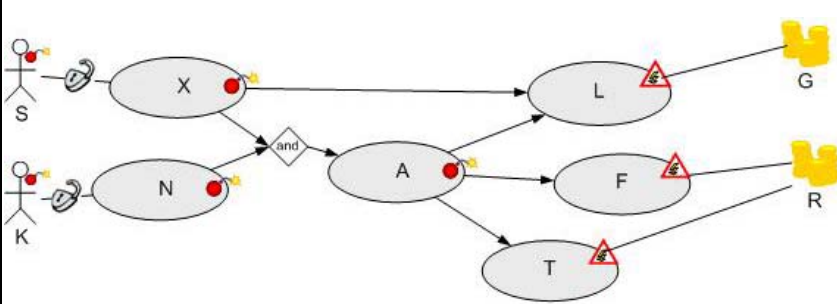


Diagram 1

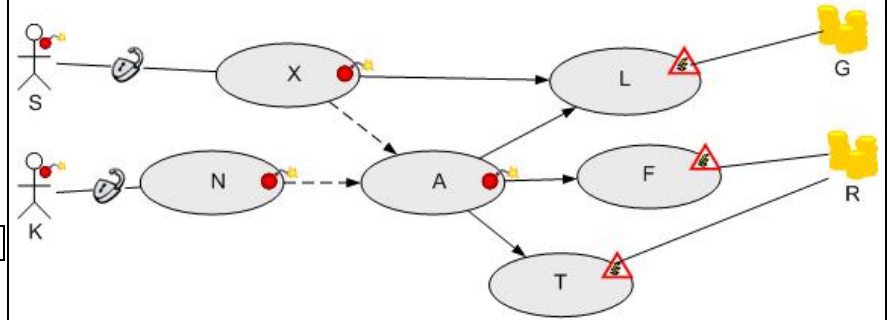
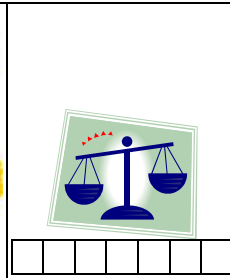


Diagram 2

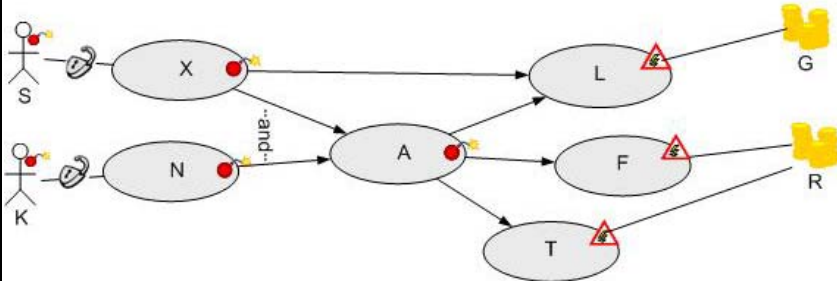


Diagram 3

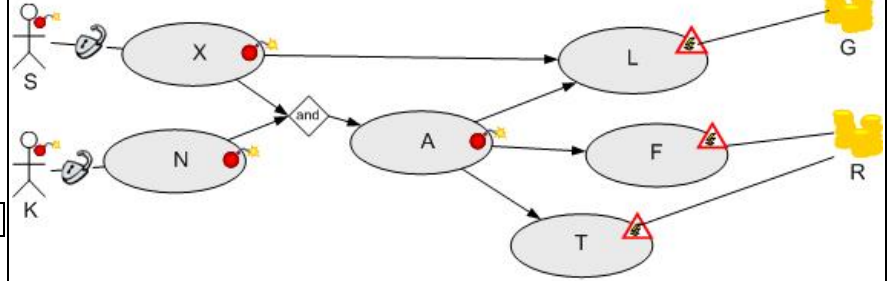
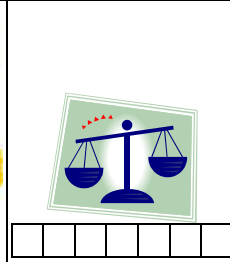


Diagram 1

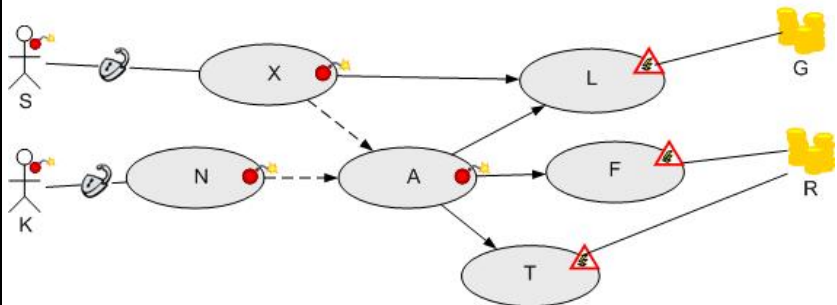


Diagram 2

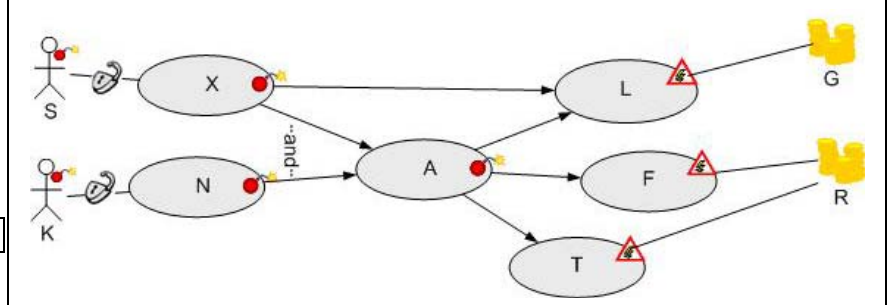
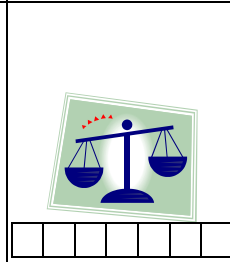
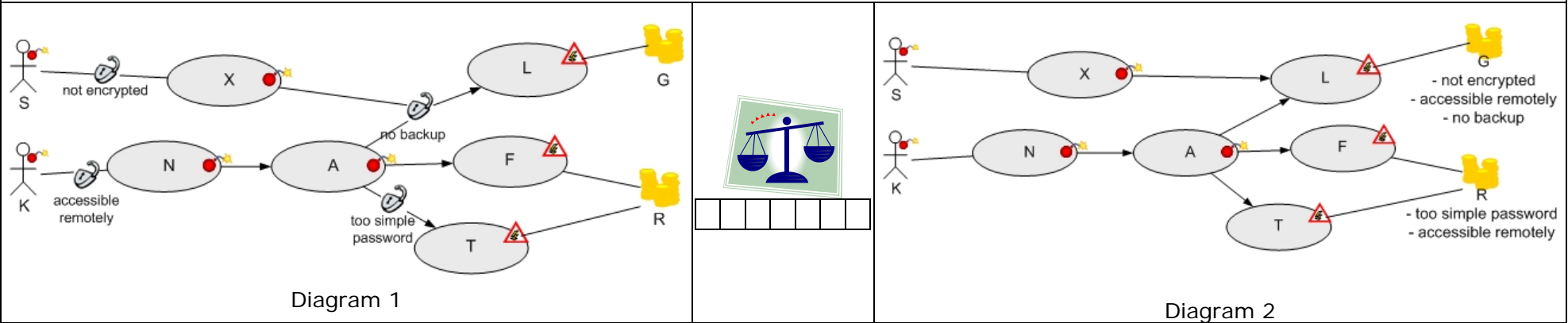


Diagram 3

12) Which diagram shows best that the asset G and R share the same vulnerability?



13) Which diagram shows best that unwanted incident F poses the largest risk for asset R?

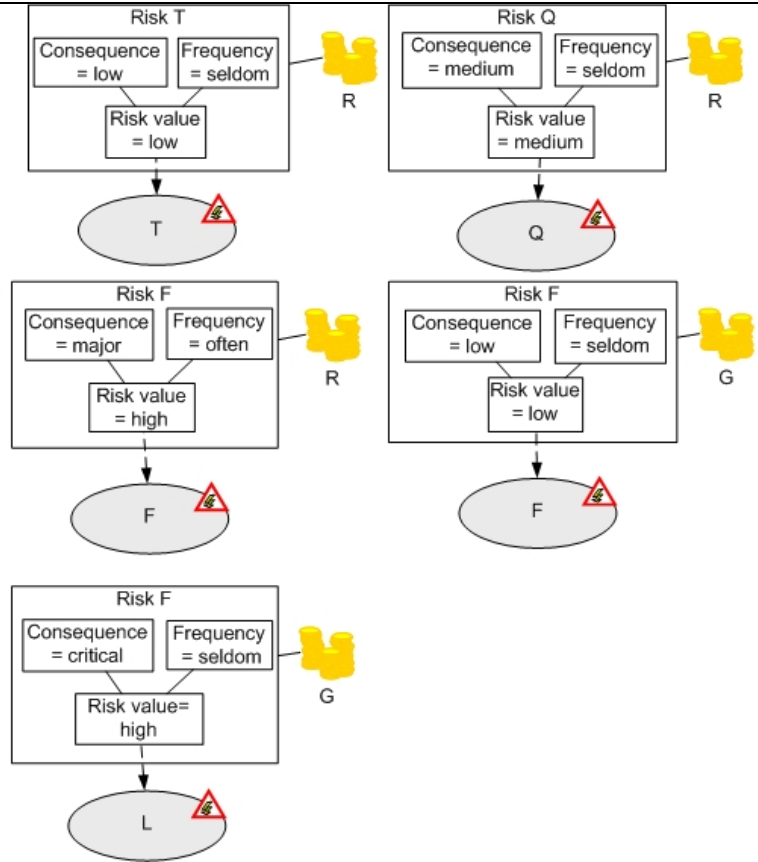


Diagram 1

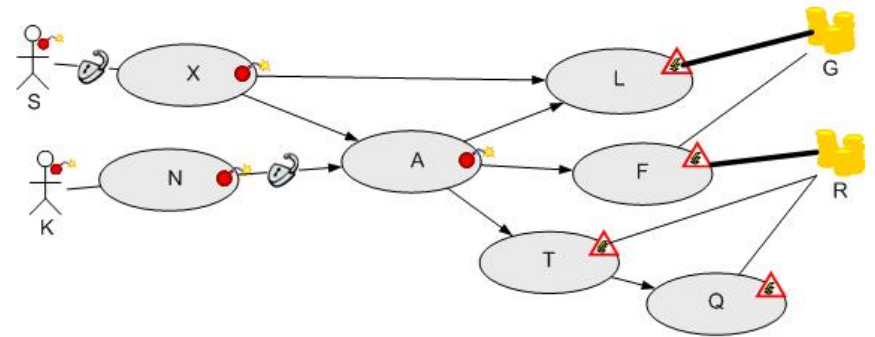


Diagram 2

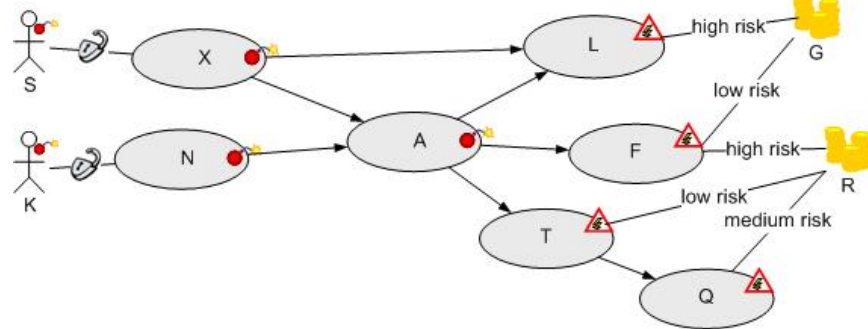


Diagram 3

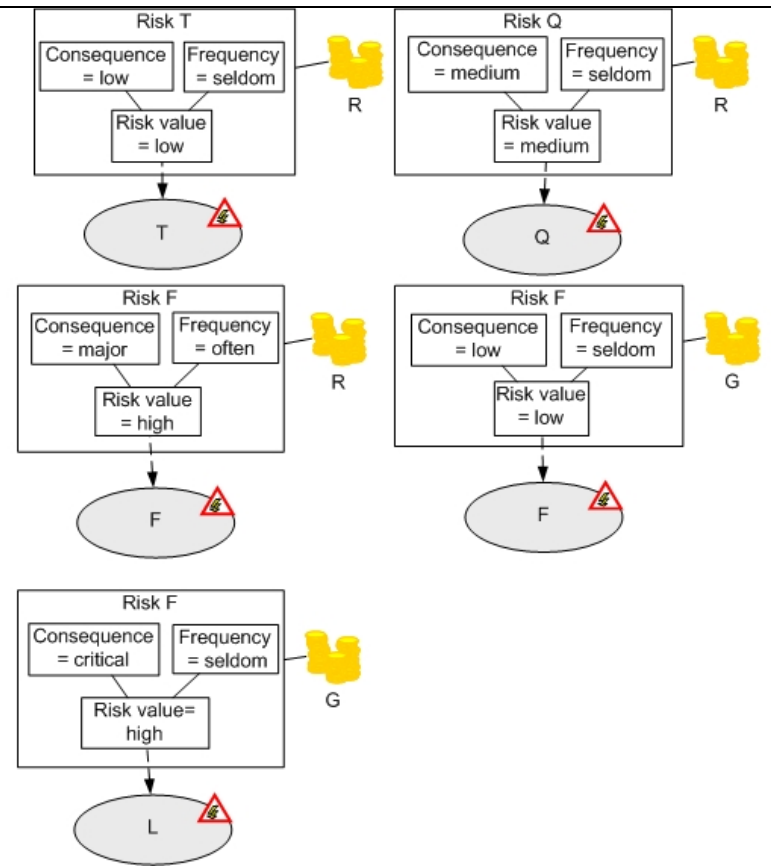
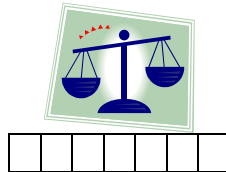


Diagram 1

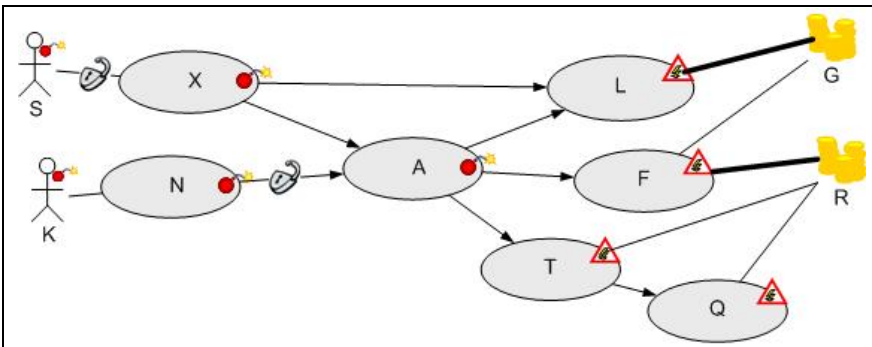


Diagram 2

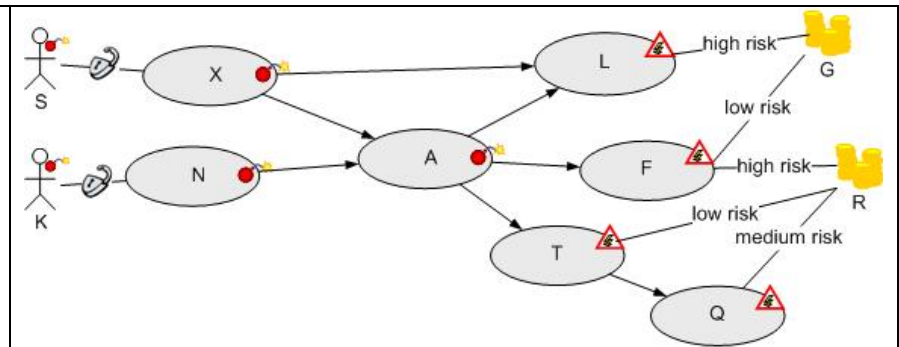
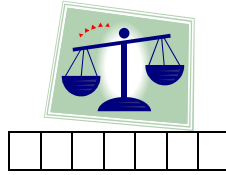


Diagram 3

14) Which diagram shows best that unwanted incident of scenario F represents two different risks?

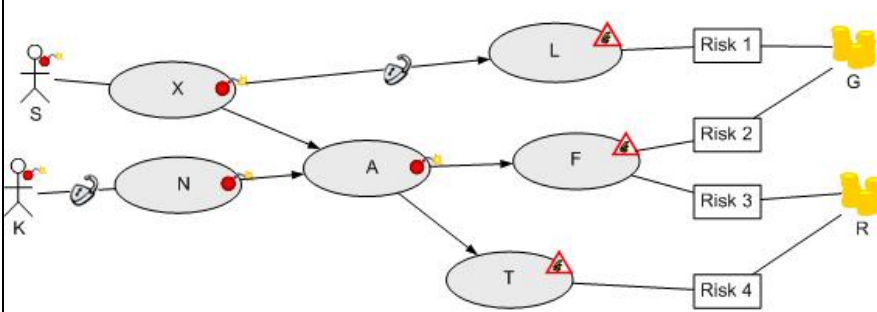


Diagram 1

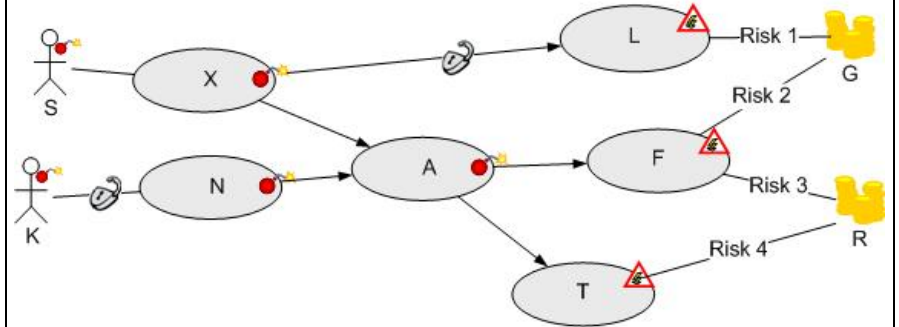
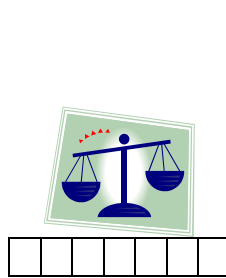


Diagram 2

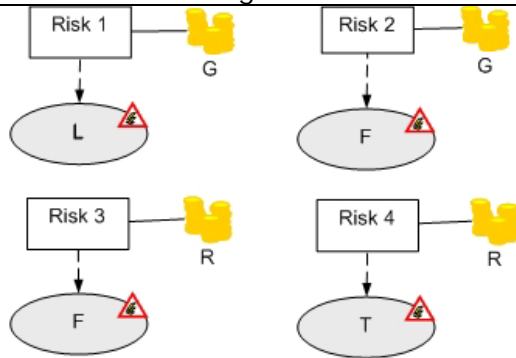


Diagram 3

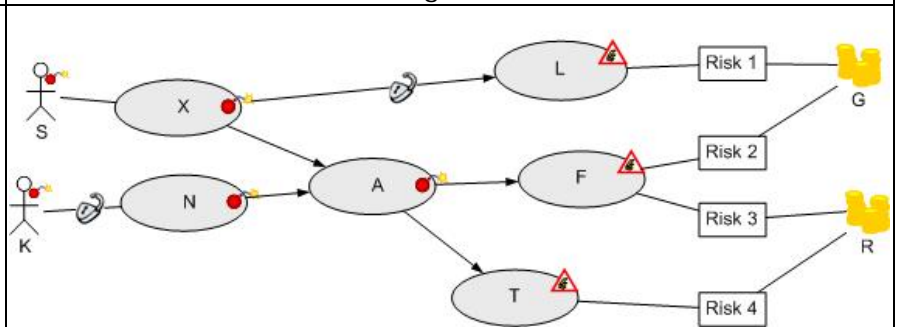
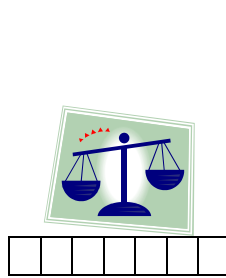


Diagram 1

