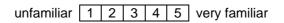
Questionnaire

This questionnaire is a part of the investigation of the general understanding of security analysis terms among people with different backgrounds. Even people with no experience in security analysis know some of the terminology because it is used in the daily language and we like to investigate which terms that are well known and which are not. The data will be valuable in our work with a graphical language we use in security analyses.

1) On a scale from 1-5, how familiar are you with risk analysis terms like asset, threat, risk, unwanted incident, consequence, probability, frequency, treatment and vulnerability?



2) If you were to participate in a security analysis, which roles could you have?

		select at least one
Ι.	The role as risk analysis leader	
II.	The role as user or intended user of the	
	system assessed	
III.	The role as expert (on one or more	
	aspects of the system)	
IV.	The role as system designer	
V.	The role as recorder of the risk analysis	
	results (secretary)	

3) What can be considered as assets in a security analysis?

		false	partly false	uncertain	partly true	true
a.	a customer register					
b.	a company brand					
C.	critical system services					
d.	human lives					
e.	equipment					
f.	source code					
g.	a company's strategies					
h.	the employees' job satisfaction					
i.	e-mail					

4) What is true about the relationship between risk and asset?

		false	partly false	uncertain	partly true	true
a.	a risk can harm or reduce the value of the asset					
	a presumption for a risk to arise is that there are nerabilities for someone to exploit					
C.	a risk will harm or reduce the value of an asset					
d.	one risk may harm more than one asset					

5) What is the difference between a risk and an incident scenario for an asset?

		false	partly false	uncertain	partly true	true
a.	an incident scenario is an actual event that can harm the asset but without a frequency or consequence value					
b.	a risk for an asset is an unwanted incident assigned a consequence and frequency value					
C.	an unwanted incident cannot be part of more than one risk					

6) The goal of a *treatment* can be:

		false	partly false	uncertain	partly true	true
a.	to reduce risk					
b.	to remove a threat					
C.	to remove a vulnerability					
d.	to reduce a threat					
e.	to remove a risk					
f.	to reduce a vulnerability					
g.	to remove an unwanted incident					
h.	to reduce an unwanted incident					

false partly false uncertain partly true true a. it is usually directed towards a vulnerability b. it is usually directed towards a threat c. it is usually directed towards an unwanted incident d. it is always directed towards a risk e. it can be directed towards both a vulnerability and threat f. it cannot be directed towards both a vulnerability and an unwanted incident at the same time g. it cannot be directed towards both a vulnerability, a threat and an unwanted incident at the same time

7) What is true about *treatment*?

8) When will a *treatment* be considered successful?

		false	partly false	uncertain	partly true	true
a.	if it reduces risk frequency					
b.	if it reduces risk consequence					
C.	if it makes the risk value acceptable					
d.	if it eliminates the risk					
e.	if it reduces both frequency and consequence					
f.	if it reduces the risk value to an acceptable level					

9) What is the relationship between frequency, likelihood and probability?

-/	,								
		false	partly false	uncertain	partly true	true			
a.	the term frequency comprises both likelihood and probability								
b.	likelihood is measured as "often, seldom, never etc."								
C.	probability is measured as "50%, 10% etc."								
d.	frequency is measured as "1, 3, 2000, 3.5 etc"								
e.	likelihood is measured as a value between 0-1								
f.	likelihood covers both frequency and probability								

10) What can be used to calculate *risk value*?

		false	partly false	uncertain	partly true	true
a.	probability and frequency					
b.	likelihood and consequence					
C.	consequence and frequency					
d.	consequence and probability					
e.	frequency and likelihood					

11) What is a *risk* composed of?

		false	partly false	uncertain	partly true	true
a.	a consequence, a frequency, a probability and an unwanted incident					
b.	a probability, an unwanted incident and a consequence					
C.	a consequence and a frequency and an unwanted incident					
d.	none of the alternatives above					

12) What is the relationship between risk and unwanted incident?

		false	partly false	uncertain	partly true	true
a.	a risk is part of an unwanted incident					
b.	a risk initiates the unwanted incident					
C.	an unwanted incident is part of a risk					
d.	an unwanted incident can be a part of more					
	than one risk					

13) When can one consider an unwanted incident a risk?

		false	partly false	uncertain	partly true	true
a.	when it has a consequence, but not necessarily a frequency					
b.	when it has a frequency, but not necessarily a					
с.	consequence when it has both a frequency and a					
	consequence			<u></u>		

14) What is true about *vulnerability*?

		false	partly false	uncertain	partly true	true
a.	it can be a weakness or lack of the asset itself					
b.	it can be a weakness or lack of the asset's					
	surroundings					
C.	a threat can exploit vulnerabilities					

15) What can be considered a *threat*?

		false	partly false	uncertain	partly true	true
a.	hardware					
b.	people					
C.	software					
d.	an event (initiated by a person)					

16) What is true about threat?

		false	partly false	uncertain	partly true	true
a.	a threat can initiate an unwanted incident					
b.	a threat can constitute a risk even if there are no vulnerabilities to exploit					
C.	a threat can potentially reduce the value of an asset					
d.	a risk is always associated with a threat					
e.	a threat is not necessarily connected to a risk					