1 **a)** IT security have a number of general goals that you almost always look at when you are evaluating and/or implementing some controls to increase security. These goals are summarized in the **CIA model**. Describe this model.

b) IT Security threats are constantly changing. Some of the recent threats we have seen are:
- Ransomware attacks
- Social engineering attacks where you try to make people authenticate (e.g. with BankID) on Internet
- Cryptocurrency botnets

Give a short description of each of these threats and what the purpose of them are.

(6+6 p)

2 **a)** Describe the three different methods **Steganography**, **Encryption** and **Digital Watermarking**? What is the purpose of each method?

b) If you were to develop an application for an organisation that is to deal with sensitive information, what **encryption algorithm** would you use? Motivate your choice.

c) Asymmetric encryption algorithms may have several different application areas (some algorithms only have one). Describe these possible application areas.

(4+4+4 p)

3 **a) Program Security** defined by the textbook have two main objectives. What are these two objectives?

b) Testing is one of many Developmental Controls for Program Security. There are different types of testing, briefly describe some of these types. There are also some problems with using testing as a control, briefly describe some of these problems.

c) One technique you can use in a program to deal with errors is **fault tolerance**. Describe what that this, how it can help with some errors and also give an example of how to use it

(4+4+4 p)

4 **a)** The Operating system is crucial for getting some level of security in a computer system. One basic technique used to get it is by separation. The most common form of separation used is **logical separation**. Describe how that type of separation works.

b) Memory protection is one of the methods applied in operating systems. Shortly describe a few methods used to implement memory protection.

c) One of the tasks for the operating system is authentication. Name four different ways to **authenticate** a person in an operating system.

(4+4+4 p)

5 **a)** In Databases you implement something called **Two-phase Update**. What is that and why do you do it?

b) What is considered to be **Sensitive data** can vary depending on many different factors. Describe some of the reasons data might be seen as Sensitive data and typical examples of Sensitive data.

c) A typical security related attack on databases is the **Inference attack**. What is the goal with such an attack and how is performed?

(4+4+4 p)

6 **a)** A security plan consists of many different areas. Describe the content of the following areas: **Policy**, **Accountability** and **Maintenance**.

b) Study the table below. You will see the details of three different risks and for each risk two possible controls. Make the calculations that will fill in all the gaps in the table and then make an argument for what controls you would advise an organisation to implement.

Risk	Control	Impact	Probability	Exposure	Cost of control	Probability after control	Exposure after reduction	Leverage	Savings
1	I	20000	0,1		200	0,095			
	II	20000	0,1		1000	0,05			
2	III	100000	0,2		10000	0,1			
	IV	100000	0,2		5000	0,2			
3	V	1000	0,8		100	0,1			
	VI	1000	0,8		200	0,2			

(6+6 p)