# EXAMINATION IN CYBER SECURITY

**October 21st, 2019 (Monday)**

## Instructions

There are two parts: Part 1 and Part 2. Part 1 consists of one question, which is in total worth five (5) points. Part 2 consists of two questions, which are in total worth thirty five (35) points. Partial credits of 0.5 points will be provided for both parts. The maximum number of points that may be accomplished is forty (40) points. In order to pass you are expected to attain at least twenty (20) points.

No books are allowed on this exam. Only answers in English will be accepted. Use the A4 papers provided in the exam room to write down your answers, only write on the front side of the paper (i.e. where your seat number, room, page count etc. are specified).
Please, note that you must clearly specify any presumptions made.
**Write eligible. Unreadable answers will be failed.**

Grading scale for each grade is as follows:
A: 90%
B: 80%
C: 70%
D: 60%
E: 55%
Fx: 50%
F: 49%

***Best wishes for a successful and profitable work. Lycka till!***

## Part 1

### Question 1 (5 points)

Explain the meaning of the following concepts (1 point each):

a) Cyber attack
b) Security vulnerability
c) Security policy
d) Security metrics
e) Penetration test

# Part 2

## Scenario Description

The international airport of Sweden, Scandinavica International Airport (SIA), is a protected national object (Swe. "skyddsobjekt") which means that the airport and its surrounding area is protected by law (Skyddslag (2010:305)) just like the Swedish Intelligence Agency (FRA) buildings, broadcasting television and radio stations, power plants, the parliament buildings and more. It is the largest airport in Sweden, situated in the capital city Stockholm, and the connection hub for most international flights to and from Sweden. SIA is constantly a subject to threats from different sources (hostile forces, terrorist, activist groups, as well as individual actors). Now consider that the following fictive and simplified scenario has taken place at SIA.

At 06:22 AM on the day of this exam, the daily malware scanner software reported that a malicious trojan with espionage capabilities was detected in one of the systems at SIA (marked with a rectangle in Figure 1).

In your role as a Security Incident Manager, take into consideration the above given scenario and the IT architecture of SIA (see Figure 1) and answer the following questions.

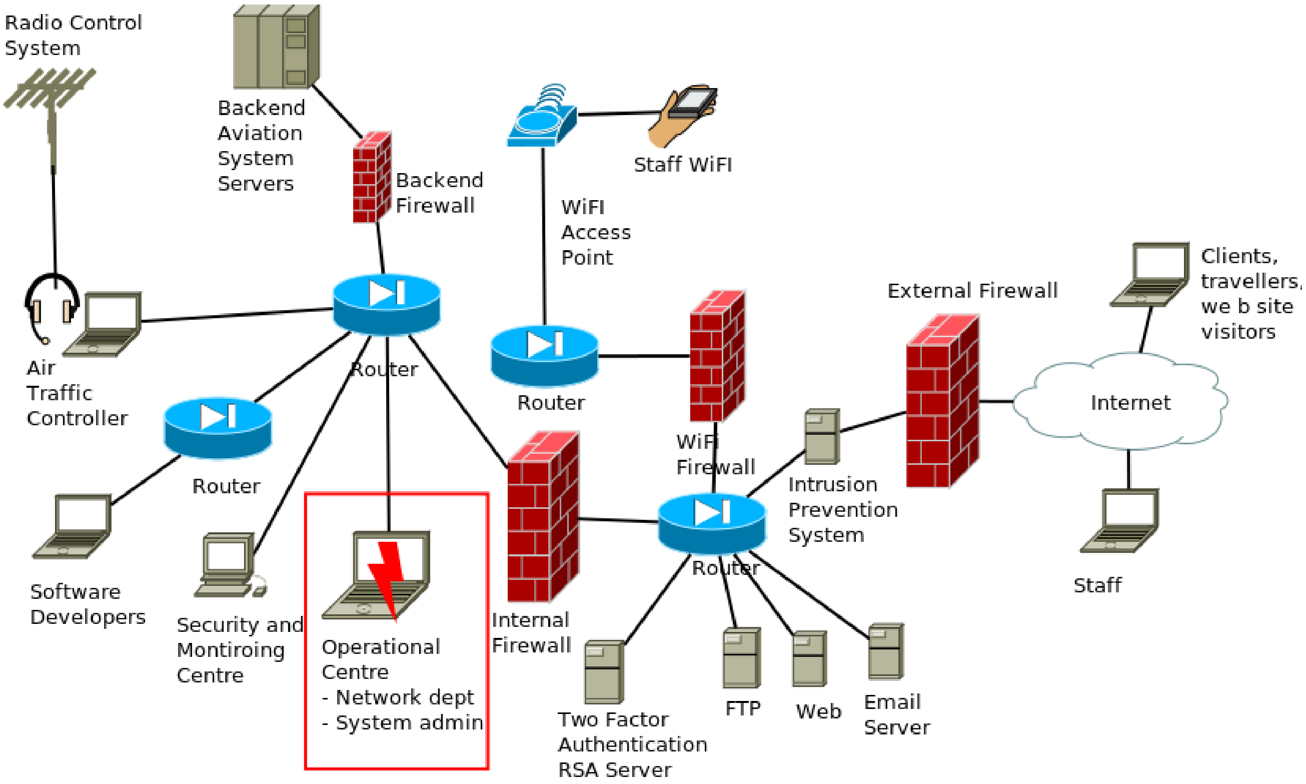

Figure 1. IT infrastructure of SIA international airport in Sweden

## Question 2 (20p).

a) Model two threats/attacks (exclude malware) identified from the above mentioned SIA scenario. (10 p)

b) Define two security metrics and identify necessary security controls that can mitigate threats identified in your answer to question 2a. Justify your answer. (10 p)

## Question 3 (15p).

a) Apply the incident response process (mentioned in the lectures/course literature of your choice) on the given SIA scenario. Consider the global, national, and organisational level aspects. (5 p)

b) Discuss how a disaster recovery should be implemented given the above mentioned SIA scenario. (5 p)

c) Describe a penetration test process and provide an example of how it can be used on the given SIA architecture? Include threats identified in answer to questions 2a. (5 p)