OMTENTAMEN i Riskanalys & IT-säkerhetssystem, 7,5 hp
IT-forens2

2011-01-03

Namn: _____

Personnummer: _____

Inga hjälpmedel tillåtna.

Del 1: Riskanalys och informationssäkerhet

Uppgift 1 Grundläggande begrepp och standarder (10 p)

a) Definiera termen ”informationstillgång” (1 p)

b) Ge tre exempel på olika typer av vanliga informationstillgångar. (2 p)

c) Definiera termen ”informationssäkerhet” (1 p)

d) Nämn tre nyckelbegrepp inom informationssäkerhet som kan användas vid informationsklassning av ett företags dokument. Vilken anser du är viktigast? Motivera! (2 p)

e) Beskriv förhållandet mellan begreppen ”informationssäkerhet” och ”IT-säkerhet” grafiskt. Vilka andra typer av säkerhet kan förekomma, och hur är de relaterade ”informationssäkerhet” och ”IT-säkerhet”? (2 p)

f) Ge två exempel på svenska informationssäkerhetsstandarder. Ange titel och nummerserie (1 p)

g) Vilket heter det förlag som ger ut standarder för informationssäkerhet i Sverige? (1 p)

Uppgift 2 - Riskanalys, begrepp och metod (10 p)

a) Definiera termen ”riskaptit” (1 p)

b) Definiera termen ”sårbarhet” (1 p)

c) Redogör för de olika stegen i en risk- och sårbarhetsanalys för informationssäkerhet. (3 p)

d) Enligt standarden för riskanalys är det viktigt att ha ett verksamhetsperspektiv: motivera varför. (1 p)

e) På vilka olika sätt går det att hantera en känd risk? (2 p)

f) Vem ska fatta beslut om vilka risker en verksamhet ska ta? (1 p)

g) Vilken roll har du som informationssäkerhetsansvarig vid beslut som rör informationssäkerhet? (1 p)

Uppgift 3 - Hot mot informationstillgångar (10 p)

a) Nämn tre reella hot mot ett företags informationstillgångar. (3 p)

b) Vad innebär begreppet ”social engineering” och vad vill angriparen åstadkomma? (2 p)

c) Beskriv minst två vanliga metoder för social engineering och hur användare kan skydda sig mot sådana attacker. (2 p)

d) Vad innebär ”säkerhet på djupet” i sammanhanget informationssäkerhet? Nämn minst fem viktiga säkerhetsfaktorer och beskriv hur de bidrar till säkerheten. (3 p)