# Instruktioner för examinationsuppgift i TSIT01 Datasäkerhetsmetoder

Uppgiften examineras efter om ni fått med följande punkter och utfört dem korrekt. Gruppens storlek påverkar krävt djup och marginaler för småfel, men alla måste ha med alla punkter.

### CIA-analys

Rapporten ska innehålla en redogörelse för vilka data som är aktuella i det valda fallet och hur känsliga de är för skador av samtliga tre typer. Det ska alltså noteras även att de eventuellt inte är känsliga, t. ex. att företagets offentliga webb-sida inte kräver något skydd alls för sekretess. För att genomföra detta steg, måste ni klargöra verksamhetens mål och krav för ert valda exempel, eftersom det är detta som styr vad som är känsligt.

### Hotanalys

Rapporten ska innehålla en redogörelse för vilka hot, som kan vara aktuella i det valda fallet. Där ska dels ingå de specifika hot som gäller just den valda situationen, dels kommentarer om mer generella hot, som allmänna nätattacker, risk för fysiska skador, som ger bristande tillgänglighet o. s. v. Inga väsentliga hot i dagens IT-värld får saknas. Rapporten får inte heller missa eventuella viktiga hot, som är specifika för det valda systemet.

### Riskanalys

Rapporten ska innehålla en värdering av de identifierade hoten efter hur sannolika de är och hur stora skador de kan ge, om inget skydd finns. Det behöver inte vara årlig riskkostnad i kronor, och när det gäller skador av typen sämre anseende är måttet kronor per år knappast ens det lämpligaste. Men det måste finnas en möjlighet att rangordna åtgärder efter hur angelägna de är, och underlaget för detta är riskanalysen.

### Bristidentifiering

Rapporten ska identifiera alla typer av brister, som kan möjliggöra att hoten verkligen resulterar i skador. Vissa av dessa brister kan kanske i en del fall betraktas som redan åtgärdade, men det ska då explicit påpekas.

### Åtgärdslista med prioritering

Rapporten ska ange vilka åtgärder, som kan vara effektiva mot identifierade brister. Varje åtgärd ska kunna motiveras av beskrivna hot och brister. För varje åtgärd ska kort anges vad den gör rent tekniskt och hur detta då ger skydd. Det räcker med en eller två meningar, men det får inte saknas. Exempel: "Brandväggen ska ge minskad risk för allmänna nätattacker. Detta åstadkoms dels genom att bara helt nödvändiga portar/tjänster släpps igenom, dels genom att bara nätadressen till filialen tillåts anropa något innanför inre brandväggen. Svar på egna anrop släpps givetvis igenom, men bara på tillåtna portar." Det räcker alltså inte att bara skriva "Brandvägg behövs som skydd mot allmänna nätattacker."

Notera att ni ska ha med alla typer av relevanta åtgärder, alltså även personalutbildning, redovisning av er behörighetsuppdelning för data och användare m. m.

Åtgärderna ska vara prioriterade efter grova uppskattningar av deras kostnad kontra angelägenhetsgrad.

### Formella krav

Det krävs inget givet format eller given kapitelindelning Det är alltså fullt möjligt att t. ex. behandla varje hot för sig, från CIA-relevans till åtgärd, bara alla punkter behandlas.