Praktisk riskanalys - en standardmetod

Margaretha Eriksson

Civ.Ing. och doktorand i informationssäkerhet KTH

irbiskonsult@tele2.se

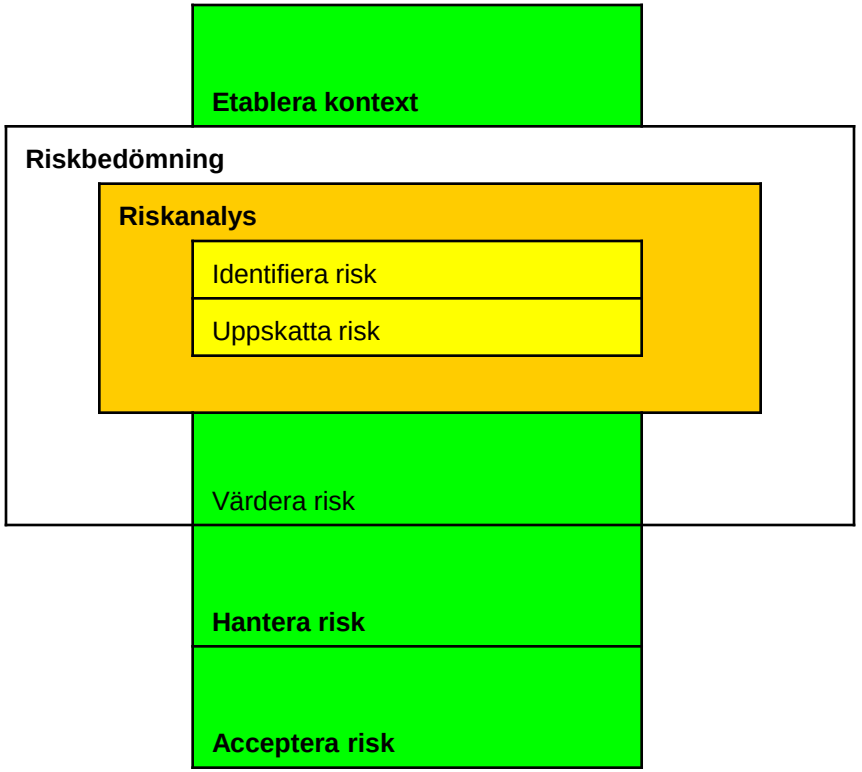
Föreläsning 6

Mål

- kunna använda risk- och sårbarhetsanalys i praktiska sammanhang
- självständigt kunna genomföra en risk- och sårbarhetsanalys

Riskhanteringsprocessen

- Etablera kontext
- Riskbedömning med riskanalys
  - Identifiera risk
  - Uppskatta risk
- Värdera risk
- Hantera risk
- Acceptera risk



Kontext - riskvärdering

Ta fram **relevant information** om informationssäkerheten i organisationen

- Grundläggande kriterier för **riskvärdering**
  - strategiska värden
  - lagar och avtal?
  - Konfidentialitet, integritet, tillgänglighet; ”CIA”
  - externa förväntningar, goodwill och renommé

Kontext - påverkan

- Kriterier för **påverkan** på
  - värdering och klassning av tillgången
  - verksamheten
  - affären och ekonomiska värden
  - planer och deadlines
  - renommé
  - efterlevnad av lagar och avtal

Kontext - riskacceptans

- Grundläggande kriterier för **riskacceptans**
  - accepteras och fastställs av högre chef
  - uppskattad vinst/uppskattad risk
  - flera riskklasser?
  - krav på framtida åtgärder?
- Verksamhetskriterier
- Lagar och föreskrifter
- Drift
- Teknik
- Ekonomi
- Sociala och humanitära faktorer

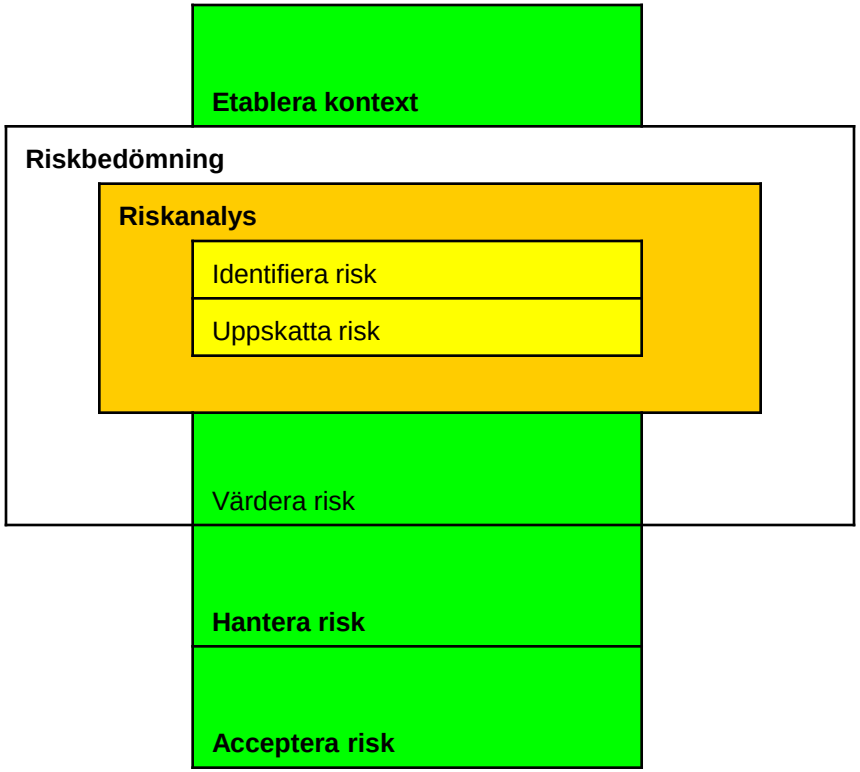
Kontext - organisation

- Process för riskhantering enl FMEA
- Roller och ansvar?
- Intressenter?
- Relation mellan organisation och intressenter?
- Eskalering av beslut
- Arkivering av redovisande dokument

OBS Denna organisation ska vara godkänd av ansvarig chef i organisationen.

Riskbedömning

- **Riskbedömning och riskanalys**
  - Identifiera risk
  - Uppskatta risk



Riskbedömning

- Identifiera, kvantifiera eller beskriv riskerna
- Prioritera m a p kriterier för
  - riskvärdering och
  - relevanta verksamhetsmål

Identifiera risker

- Händelse som kan leda till skada
- Hur, var och varför?

Identifiera värdefulla tillgångar

Identifiera värdefulla tillgångar som behöver skyddas i lista:

- Namn på tillgång
- Ägare
- Plats
- Funktion

Identifiera hot

Identifiera hot mot värdefulla tillgångar

- Information från
  - incidenter
  - systemägare
  - användare
  - hotkataloger (”levande” innehåll)
- Varifrån (källa)

Identifiera sårbarheter

- Identifiera sårbarheter inom
  - organisation,
  - processer och rutiner,
  - hanteringsrutiner,
  - personal,
  - fysisk miljö,
  - konfiguration av info-system,
  - maskin- och programvara,
  - kommunikationsutrustning,
  - externa parter
- Identifiera befintliga och planerade säkerhetsåtgärder
- Identifiera konsekvenserna m a p ”CIA”

Resultat

Lista med incidentscenarier med konsekvenser för tillgångar och verksamhet

Uppskatta risk

- Kvalitativ
  (Låg, Mellan, Hög)
- Kvantitativ
  (t ex 1-10-skala eller kostnad)

Uppskatta konsekvenser

Använd listan med incidentscenarier

- Tillgångens ersättningsvärde? (återställning/ersättning av information)
- Konsekvenser för verksamheten?

Bedöm sannolikhet för incidentscenario

- Bedöm sannolikheten för varje scenario baserat på
  - erfarenhet
  - statistiska underlag
- Avsiktliga hotkällor
  - motiv och förmåga hos angripare
  - attraktionsvärde
- Oavsiktliga hotkällor
  - geografiska faktorer som
    extremt väder, vulkanutbrott, mänskliga fel, etc
- Sårbarheter
- Befintliga säkerhetsåtgärder och hur effektiva de är

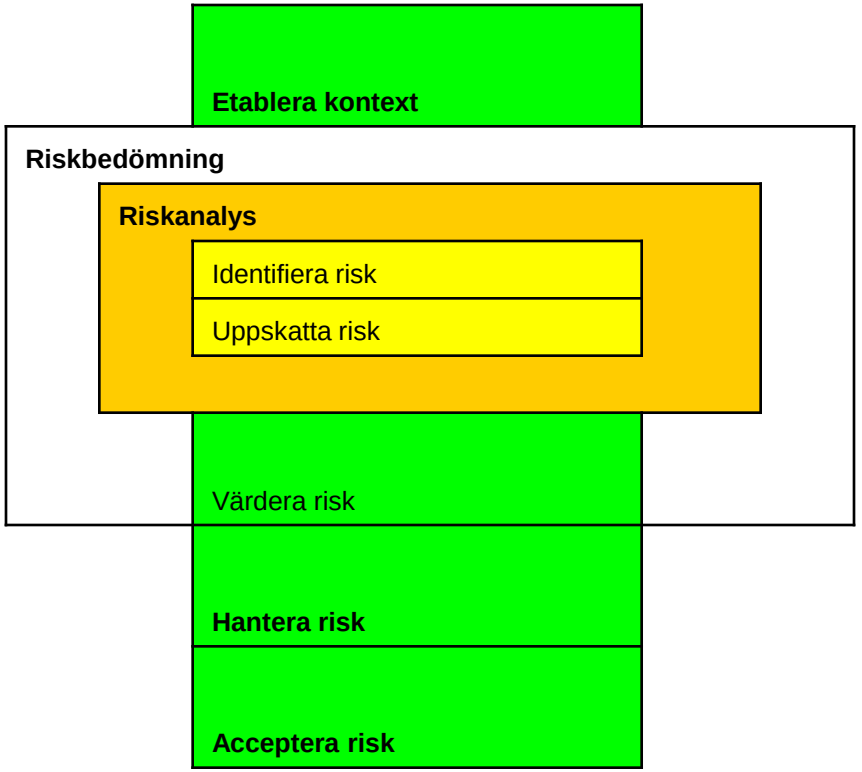
Nivå för uppskattad risk

Uppskattad risk =

Sannolikhet för incidentscenario **x** Konsekvens

Värdera risk

- Etablera kontext
- Riskbedömning med riskanalys
- **Värdera risk**
- Hantera risk
- Acceptera risk



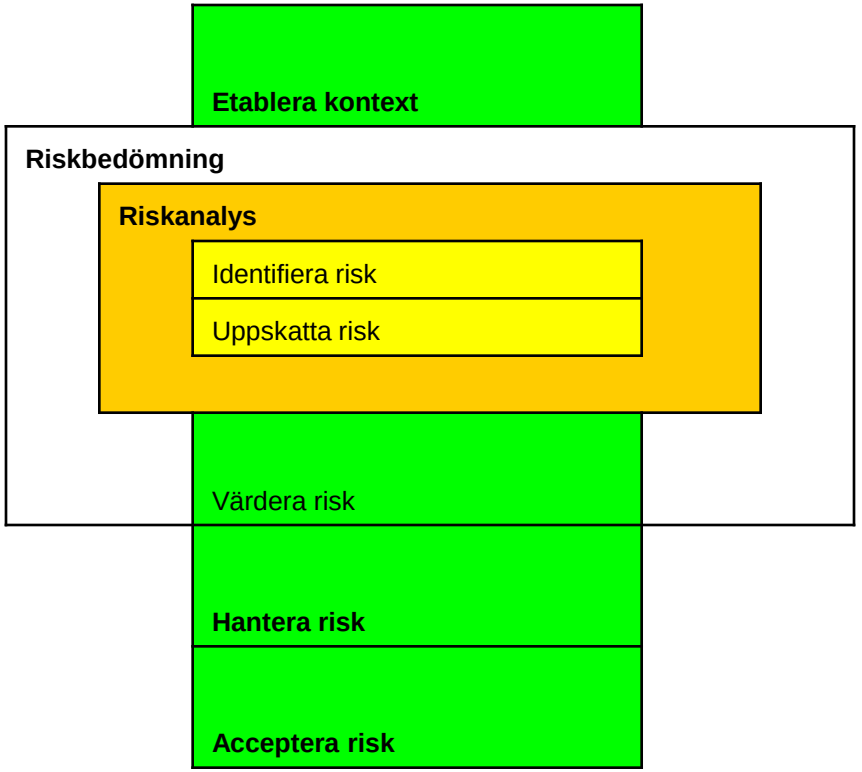
Värdera risk

- Jämför risknivåerna med
  - kriterierna för riskvärdering
  - kriterierna för riskacceptans
- Är kriterierna relevanta?
- Är processen viktig?

- Besluta om aktiviteter och prioriteringar

Hantera risk

- Etablera kontext
- Riskbedömning med riskanalys
- Värdera risk
- **Hantera risk**
- Acceptera risk



Hantera risk

- Säkerhetsåtgärder för att
  - reducera,
  - bibehålla,
  - undvika, eller
  - överföra risker
- Definiera plan för riskhantering

- Chefen ska acceptera risken

Praktisk risk- och sårbarhetsanalys

Om seminarieuppgiften

- Förstasidan:
  Seminarieuppgift i Riskanalys och informationssäkerhet, vt 2012.
  Gruppnummer
  Gruppmedlemmar med namn och personnummer

RS-rapporten

- Vem ska läsa den?
- Målgrupp - chefer eller tekniker?
- Kortfattad, inte längre än nödvändigt (Det är en rapport, inte uppsats!)

Rapportens rubriker

- Kort beskrivning
- Bakgrund
- Område
- Inblandad teknik/utrustning
- Inblandande personer
- Vem äger problemet?
- Scenario/case
- Konsekvenser
- Riskbedömning
- Hur riskerna hanteras

Miniexempel

- **Kort beskrivning:** ”Nyckelkorten till lokaltrafiken använder en vanlig magnetremsa för att lagra information, och denna kan enkelt kopieras.”
- **Bakgrund:** ”1999 investerade lokaltrafiken i ett nytt biljettsystem. Detta biljettsystem var digitaliserat, till skillnad mot det tidigare som använde poletter…”
- **Område:** ”Lokaltrafik/nyckelkort.”
- **Inblandad teknik/utrustning:** ”Nyckelkort, biljett, magnetremsa, biljettläsare”.
- **Inblandade personer:** ”Passagerare, förare, kontrollant.”
- **Vem äger problemet:** ”Lokaltrafikens IT-avdelning som köpt in ett dåligt biljettsystem”

Miniexempel (forts.)

- **Konsekvens:** ”Genom att inte ha unika biljetter som enkelt kan kontrolleras är det omöjligt att ha kontroll på biljettanvändandet i lokaltrafiken i stad XXXX”.
- **Riskbedömning:**
  Hur riskbedömning skett i detta fall: Varför detta sätt att bedöma risk är rimligt i detta fall: Värdering:
  Prioritering:
  Åtgärdsplan:
- **Hur riskerna kan hanteras:**
  Diskussion:
  (Kring uppgiften i stort, vad som har gått bra, vad som kunde ha gått bättre)

Läs mera i...

- ISO/IEC 27005:2008 Informationstekniker – Riskhantering för informationssäkerhet
- Säkerhetshuset,
  Handbok 3, Säkerhetsanalys
- LIS, Ledningssystem för informationssäkerhet
  www.informationssakerhet.se