



Riskanalys

IT i hälso- och sjukvården
(17 sidor)

1

Riskanalys

- Är en systematisk riskbedömning
- Kan stödjas av metoder och verktyg
- Kan avse hela eller delar av verksamheten eller hela eller delar av informationssystem

2

Risikanalys - faser

1. Avgränsa analysområde
2. Identifiera informationstillgångar
3. Identifiera möjliga hot
4. Bedöm sannolikhet & bedöm potentiell skada
5. Värdera risken
6. Kan risken accepteras?
 - Om ja → Ingen åtgärd
 - Om nej → Åtgärder

3

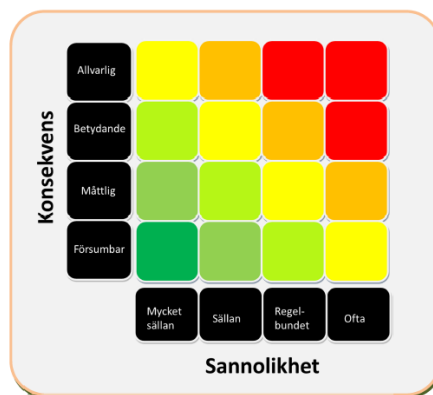
1 Avgränsning

- Verksamhetsanalys
 - För att identifiera känslig information i och utanför IT-baserade system
 - Gemensamgöra olika uppfattningar
- Analysobjektets omfattning
 - Egen verksamhet, ibland även samarbetspartners
 - Hela eller delar av verksamheten
 - Nya områden i verksamhet

4

4 Bedömning av sannolikhet

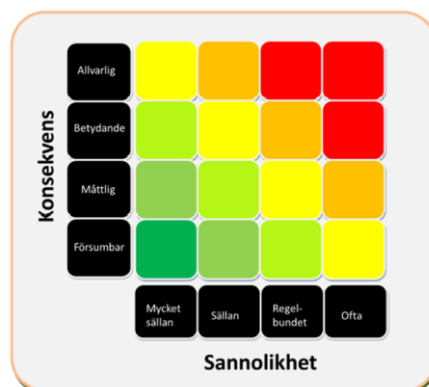
- Kvantitativ
 - Sannolikhet 0-1
 - Frekvens (antal ggr/tidsperiod)
- Kvalitativ bedömning
 - Kategorier
 - Mycket sällan
 - Sällan
 - Regelbundet
 - Ofta



7

4 Bedömning av skador

- Kvantitativ bedömning av skador
 - Belopp i kr
 - % av omsättning
- Kvalitativ bedömning av skador
 - Kategorier
 - Allvarlig
 - Betydande
 - Måttlig
 - Försumbar



8

5 Värdera risk

- Kvantitativ bedömning av risk
- Kvalitativ bedömning av risk

- För att kunna göra en kvantitativ bedömning av risk måste BÅDE sannolikheten och skadan vara kvantitativa. Om den ena delen eller båda är kvalitativa blir riskbedömningen kvalitativ.

9

6 Riskacceptans

- Accepteras risken?
- Om ja, ingen åtgärd
- Om nej, åtgärd



10

7 Bestämma åtgärder

- Redovisa åtgärdsförslagets effekt
 - Mycket hög
 - Hög
 - Begränsad
 - Låg
- Typ av säkerhetsmekanism, tex
 - Förebyggande
 - Avvärjande
 - Skadereducerande
 - Återställande

11

Exempel: hotell - informationstillgångar

- Känslig information: beläggningen, snittpris, avtalspriser, volymen från respektive avtal
- Personalen och deras kompetens
- Bokningssystem
- Lagerinformation
- Budget
- Intranät
- Informationshanterade resurser: nätverk, program, datorer, fax, kopiator...

12

Exempel: hotell - Hot

- Brand, vattenskador, åska,
- Fel i IT-systemen
- Personal som sprider känslig information, t.ex. lösenord
- Ledningsgruppen sprider information
- Glömmer att uppdatera system
- Om bokningssystemet kraschar
- Hackers och crackers
- Virus

13

Exempel: hotell – Sannolikhet hot, → incident

- Personal sprida information. Beror på lojalitet. Avsiktlig - oavsiktlig.
- Ledningsgruppen sprider information – liten risk
- IT-system kraschar – liten
- Bokningssystemet kraschar - sällan
- Informationshanterande resurser skadas – regelbundet
- ...

14

Exempel: hotell – vilka skador

- Personalen sprider känslig information - måttlig
- Informationshanterande resurser skadas – regelbundet - måttliga
- Bokningssystemet kraschar – allvarliga ekonomiska konsekvenser

15

Exempel: hotell – acceptera risken?

- Dela information – accepteras
- Polycys och säkerhetsregler inte fungerar – accepteras ej

16

Exempel: hotell – åtgärder

- Förebyggande skydd för det som ej accepteras
– utbildning om IT
- Märk känslig information med ”konfidentiellt”
- Säkerhetskopiering