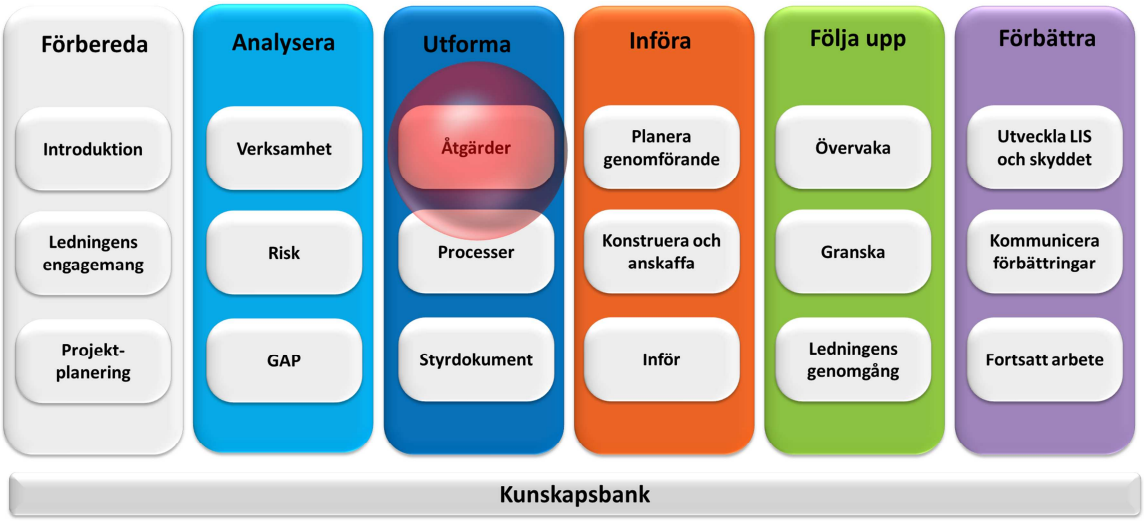
Myndigheten för samhällsskydd och beredskap

Välja säkerhetsåtgärder



Det här dokumentet är en del av metodstödet som finns att tillgå på www.informationssäkerhet.se

Författare
Helena Andersson, MSB
Jan-Olof Andersson, RPS
Fredrik Björck, MSB konsult (Visente)
Martin Eriksson, MSB
Rebecca Eriksson, RPS
Robert Lundberg, MSB
Michael Patrickson, MSB
Kristina Starkerud, FRA

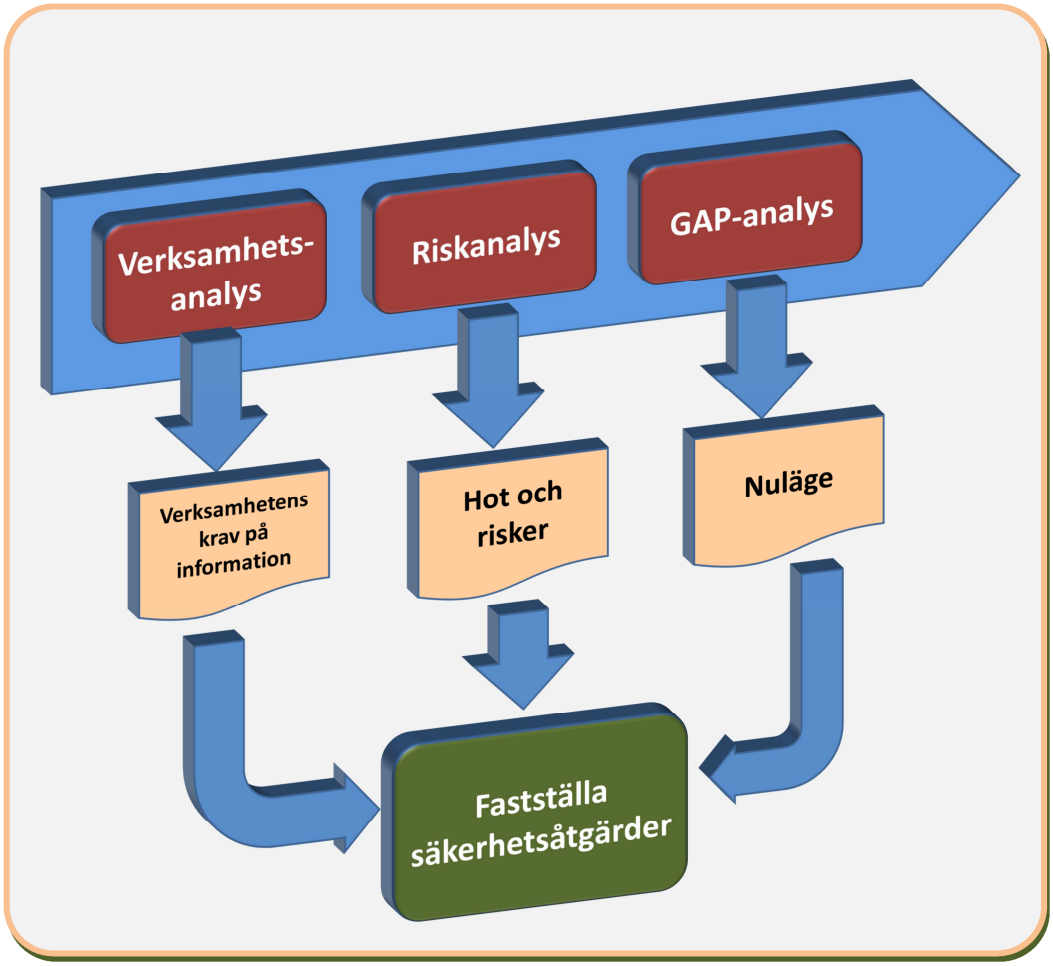
Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

1. Inledning

Syftet med det här dokumentet är att beskriva hur resultaten från de grundläggande analyserna (verksamhetsanalys, riskanalys och gapanalys) används för att bestämma vilka säkerhetsåtgärder som ska införas i verksamheten.

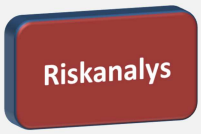
Figur 1. Analysresultaten används för att fastställa lämpliga säkerhetsåtgärder



1.1 Förberedande arbete

De grundläggande analyserna visar det aktuella säkerhetsläget och ger den kunskap som behövs för att avgöra vad som bör göras för att få en balanserad informationssäkerhet:

Verksamhetsanalysen visar både vilka informationstillgångar som ska skyddas och vilka krav det finns på skyddet. Denna kunskap påverkar valet av *vilka* säkerhetsåtgärder man ska införa, men också *hur* man inför dem, alltså omfattningen och djupet.



Riskanalysen kan visa att det behövs *direkta säkerhetsåtgärder* som ska införas på en gång för att möta en specifik risk. Den som ska fastställa säkerhetsåtgärderna behöver därför ha tillgång till rapporten från riskanalysen.

Gap-analysen visar hur den befintliga informationssäkerheten fungerar samt identifierar och värderar gapet mellan den uppmätta säkerhetsnivån och den norm som anges i standarderna ISO 27001 och 27002. Analysen visar alltså direkt vilka säkerhetsåtgärder som redan är införda och hur de står sig i förhållande till standardens norm.

1.2 Säkerhetsåtgärd

Alla verksamheter behöver vissa *säkerhetsåtgärder* för att ha en god informationssäkerhet. En säkerhetsåtgärd införs för att minska de risker som kom fram under riskanalysen och gapanalysen och det finns olika slags åtgärder.

Exempel på säkerhetsåtgärder:

- dokument som ska tas fram
- analyser som ska utföras
- tekniskt skydd som ska införas (till exempel brandvägg och intrångsdetektering)
- utbildningar som ska genomföras.

Dessutom måste man ibland ta fram eller ändra *administrativa processer* för att säkerställa god informationssäkerhet. Detta behandlas närmare i dokumentet ”Utforma säkerhetsprocesser”.

1.3 Arbetsuppgifter

För att fastställa de nödvändiga säkerhetsåtgärderna är det främst två saker som behöver göras:

1. Välja säkerhetsåtgärder
2. Dokumentera valet

Den första uppgiften passar bäst för analysledaren som gjorde de grundläggande analyserna. Han eller hon har redan intervjuat ansvariga personer för många av verksamhetens områden och har därför redan en bild av vad som bör införas och vad som kan vänta. Det kan dock bli aktuellt med kompletterande intervjuer eller seminarier.

I nästa steg är det LIS-projektets styrgrupp som ska bestämma vilka åtgärder som ska sättas in samt dokumentera detta val.

2. Välj säkerhetsåtgärder

2.1 Principer för val av säkerhetsåtgärder

Det finns två olika synsätt på hur man bäst väljer lämpliga säkerhetsåtgärder. Antingen väljer man utifrån *best practice* (bästa praxis) eller också utifrån riskanalysen.

1. **Utifrån *best practice***: Standarden 27002 listar 133 olika säkerhetsåtgärder som passar för många olika verksamheter. På så sätt kan man utgå från listans beskrivningar av säkerhetsåtgärderna och avgöra vilka som passar den egna organisationen.

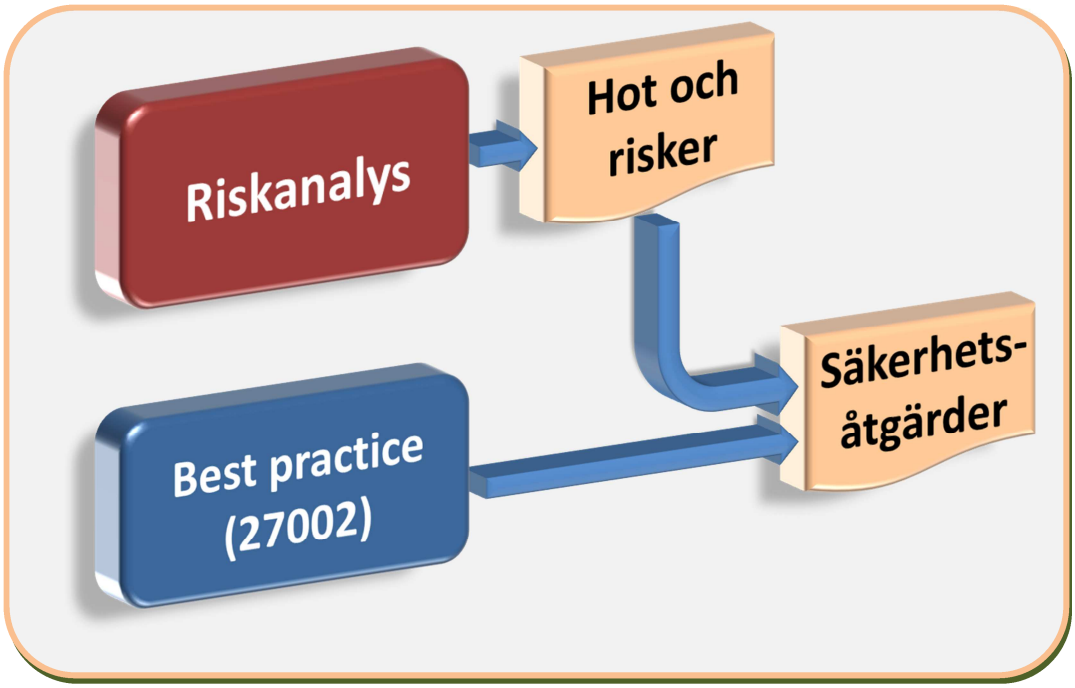
2. **Utifrån riskanalys**: Riskanalysen ger en bild av verksamhetens informationstillgångar och skyddsbehov. Med hjälp av den kan man skräddarsy säkerhetsåtgärder som passar verksamhetens specifika behov. Då används alltså inte listan med säkerhetsåtgärder i standarden 27002.

Problemet med den första metoden är att standardens lista på säkerhetsåtgärder inte passar alla verksamheter i praktiken. För vissa verksamheter saknas viktiga åtgärder medan listan innehåller åtgärder som är onödiga för andra och som i de fallen kostar mer än vad de gör nytta.

Den andra metoden, när man utgår från riskanalysen, kräver att man lyckas identifiera *alla* viktiga informationstillgångar och *alla* relevanta hot och risker, samt att man själv kan ta fram relevanta säkerhetsåtgärder som svar på dessa. Erfarenheten visar att detta ofta är svårt.

Det bästa och mest effektiva sättet är att *kombinera* de två metoderna (figur 2) för att få det bästa av två världar. Man drar nytta av kunskapen som är samlad på listan med säkerhetsåtgärder (i standarden 27002) och kan samtidigt beakta verksamhetens specifika situation och skyddsbehov (utifrån riskanalysen). Redogörelsen nedan beskriver den här kombinerade metoden. Kombinationsmetoden är vedertagen och krävs exempelvis av de verksamheter som vill få en oberoende certifiering av sin informationssäkerhet i enlighet med standarden 27001.

Figur 2. Källor till säkerhetsåtgärder



2.2 Faktorer som påverkar valet

För att välja säkerhetsåtgärder bör man främst ta ställning till

1) behovet av skydd
2) åtgärdens kostnad
3) åtgärdens förväntade effekt
4) alternativa åtgärder och investeringar.

Först måste man övergripande bedöma ifall säkerhetsåtgärden behövs eller inte, men utan att göra någon prioritering. Det kan dröja innan en vald säkerhetsåtgärd är införd; på den tiden kan mycket hända och det finns många faktorer som påverkar hur åtgärden fungerar i praktiken. Det som såg ut att vara en lysande idé kan visa sig fungera dåligt, och tvärtom. Därför börjar man med att bestämma att en säkerhetsåtgärd ska införas – inte *hur* den ska införas. Troligen finns det dock redan idéer om hur åtgärden bör vara utformad.

2.3 Välj säkerhetsåtgärder

Både riskanalysen och gapanalysen pekar på säkerhetsåtgärder som verksamheten kan välja att införa. En bra utgångspunkt är att först titta på de säkerhetsåtgärder som gapanalysen efterfrågade, och som följer 27002 (best practice):

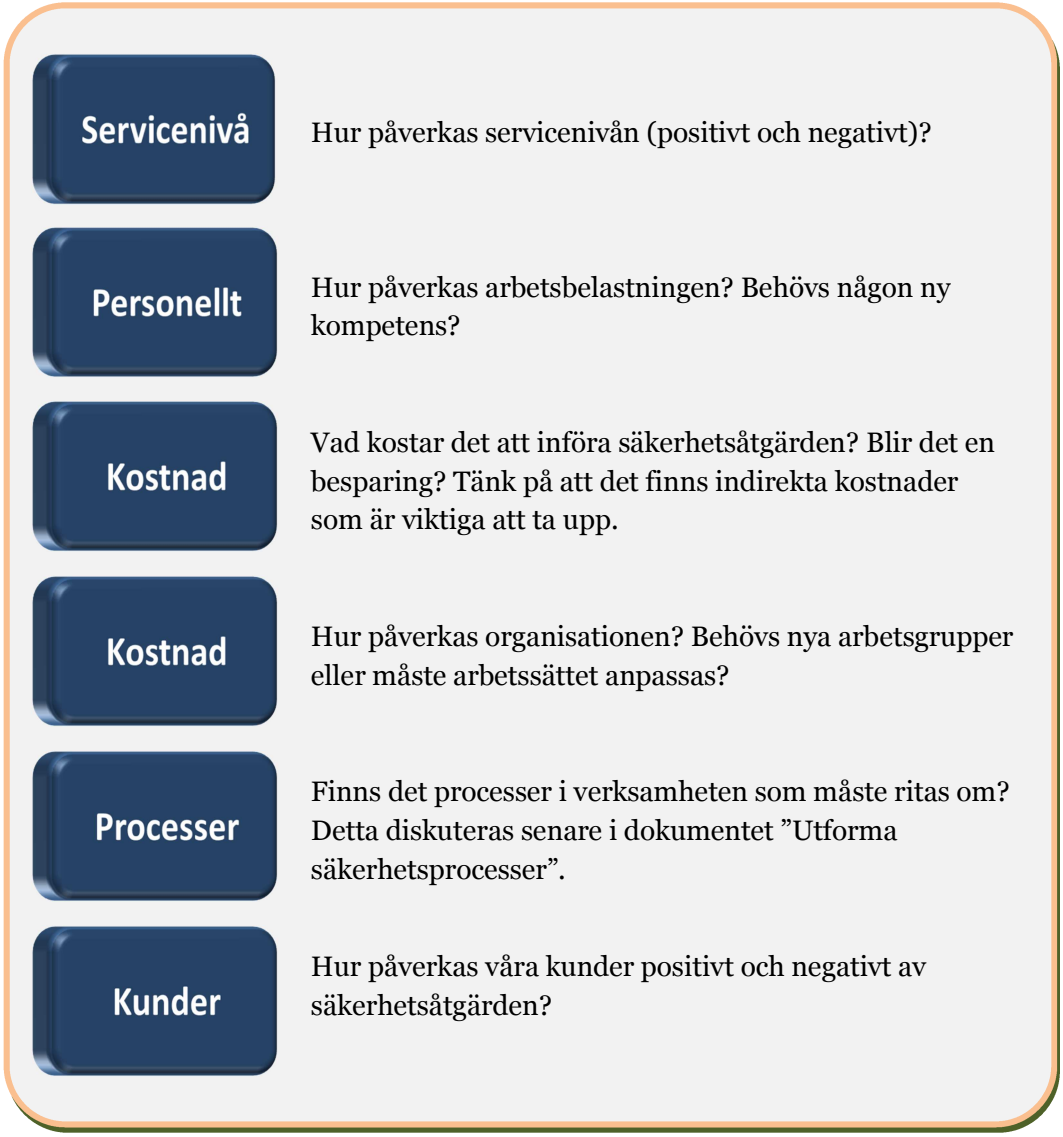
- Vilka av dessa åtgärder finns redan på plats?
- Med tanke på analysresultaten – vilka åtgärder bör finnas på plats?

Det går att välja säkerhetsåtgärder genom att helt enkelt ”kryssa” för eller lista de säkerhetsåtgärder som man vill ha med i sitt ledningssystem. Därefter kompletterar man listan med de säkerhetsåtgärder som kommer direkt från riskanalysen, ifall de inte redan finns beskrivna i 27002.

2.4 Analysera konsekvenserna

Det är viktigt att beskriva den positiva och negativa påverkan som en säkerhetsåtgärd har eftersom det då blir lättare för ledningen att förstå konsekvenserna. Detta bör beskrivas på samma ställe som valet av säkerhetsåtgärder, och med hjälp av ledorden nedan.

Figur 3. Ledord för konsekvensanalys



Konsekvensanalysen kan gälla en enskild säkerhetsåtgärd, en grupp av säkerhetsåtgärder, eller alla säkerhetsåtgärder tillsammans.

2.5 Förankra valet av säkerhetsåtgärder

Det är viktigt att förankra de valda säkerhetsåtgärderna i verksamhetens olika delar. Detta för att undvika negativa dialoger inför beslutet. Information kan skickas ut för remiss eller så kan de som påverkas av säkerhetsåtgärderna bjudas in till ett möte.

Det är viktigt att förankra åtgärderna i både den formella och den informella ledningsstrukturen. Det kan även vara bra att få fackföreningarnas syn på de valda åtgärderna, speciellt om åtgärderna innefattar loggning och övervakning av medarbetare.

3. Dokumentera valet

3.1 Syfte med dokumentation

Valet av säkerhetsåtgärder ska dokumenteras noga. För det första är dokumentationen ett viktigt underlag när säkerhetsåtgärden ska utformas och införas. För det andra är dokumentationen viktig när organisationen kommunicerar med andra parter om informationssäkerhetens upplägg, till exempel vid olika revisioner. En certifieringsrevision mot 27001 kräver bland annat att man har denna typ av dokumentation.

3.2 Olika dokumentationssätt

Det finns tre huvudsakliga sätt att dokumentera valet av säkerhetsåtgärder:

1. Markera valet direkt i gapanalysens dokumentation.
2. Beskriv valet i separat dokument.
3. Ange kort att man inför samtliga åtgärder som föreslås i 27002 (det är ovanligt).

3.3 Dokumentationens innehåll

Dokumentationen för varje säkerhetsåtgärd bör innehålla:

- **Namn**: Åtgärdens benämning
- **Ansvar**: Vilken person eller funktion som är ansvarig för den
- **Motiv**: Varför åtgärden behövs (eller varför den valts bort)
- **Påverkan**: Positiva och negativa effekter av åtgärden

En del organisationer vill att ledningssystemet för informationssäkerhet ska vara certifierbart mot ISO/IEC 27001. Då måste valet av säkerhetsåtgärder dokumenteras i en tabell eller lista med en förklaring till varför vissa åtgärder har valts, valts bort eller lagts till, med utgångspunkt i standarden 27002:s föreslagna säkerhetsåtgärder. Denna information kallas i certifieringssammanhang för ”Uttalande om tillämplighet”.

4. Nästa steg

När säkerhetsåtgärderna är valda är det dags att utforma de säkerhetsprocesser som följer av valet.