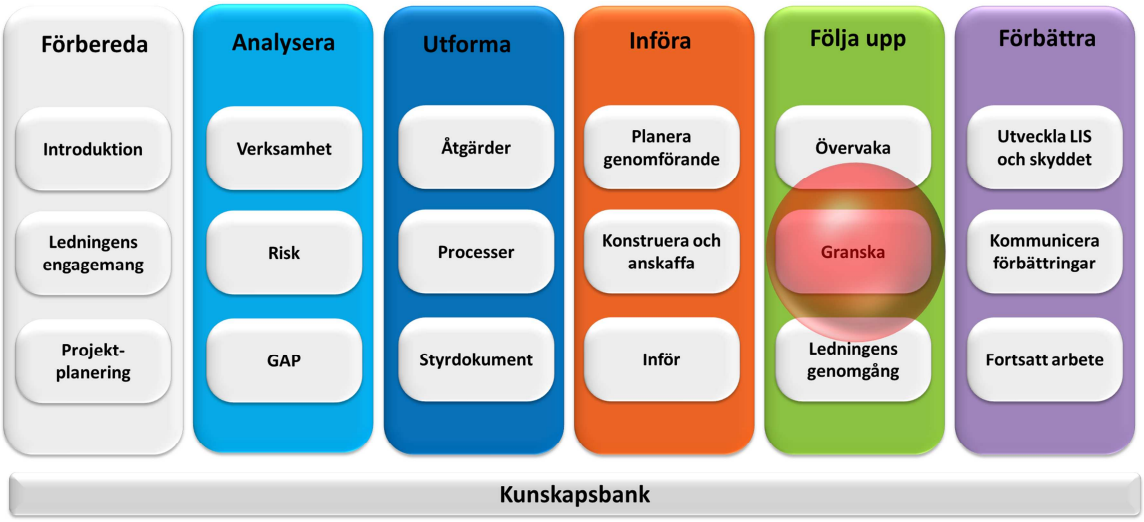
Myndigheten för samhällsskydd och beredskap

# Granska




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

Ledningssystemet rullar nu för fullt. Alla säkerhetsåtgärder och säkerhetsprocesser finns på plats och verksamheten övervakar också om allting fungerar som det ska. Men det räcker inte att bara övervaka – vissa av säkerhetsåtgärderna och säkerhetsprocesserna i verksamheten måste också analyseras mer ingående. Det är dessa analyser som faller under aktiviteten granska.

Granskning kan innebära många olika saker och man kan egentligen granska alla delar av informationssäkerheten och ledningssystemet. Det viktiga är att granskningen har ett syfte och en planering. Granskningen är en naturlig och viktig del av verksamhetsuppföljningen och de aktiviteterna bör planeras in tillsammans med andra aktiviteter i verksamhetsplaneringen.

**Egen granskning**

Granskningen som beskrivs i det här dokumentet är den som verksamheten sköter själv – inom ramen för en internrevision eller på något annat sätt. Det finns externa revisions- och granskningsorgan som också kan granska en verksamhet, men den formen av granskning ingår inte här.

Uppföljningens och därmed granskningens yttersta syfte är att förbättra verksamheten genom att följa upp, granska och analysera hur den fungerar. Ofta följer man upp i vilken utsträckning verksamheten lyckas nå de uppsatta målen.

I kravstandarden ISO 27001 framgår att själva ledningssystemets funktion ska granskas regelbundet, liksom riskbedömningarna, alla kvarvarande risker och den risknivå man har fastställt som godtagbar. Organisationen ska också göra interna revisioner av ledningssystemet.

Information från steget ”Övervaka” som föregår detta steg är en viktig källa till data och uppgifter om hur informationssäkerheten fungerar.

# 2. Typer av granskning

Man kan granska i princip allt och därmed finns det också många olika sätt att granska saker. Granskningar inom ramen för informationssäkerhet och LIS kan grovt delas in i *tekniska* och *administrativa* granskningar.

**Exempel på tekniska granskningar:**

- nätverk
- servrar
- datorer
- specifika applikationer
- egna utvecklingsprojekt

**Exempel på administrativa granskningar:**

- formella krav på ledningssystem
- efterlevnad av lagkrav
- ledningssystemets dokumentation
- metodik i egna utvecklingsprojekt

De tekniska granskningarna ser främst på insamlad loggdata medan de administrativa granskningarna bygger mer på intervjuer och på att studera dokumentation och lagar.

Standarden 27001 kräver att interna revisioner av LIS genomförs med planerade intervall. Syftet är att avgöra om alla mål, åtgärder, processer och rutiner stämmer med de interna och externa kraven samt fungerar på ett bra och förväntat sätt.

# 3. Planera granskningar

## 3.1 Internrevisionsplan

Det är bra att planera in vilka granskningar som ska göras under det kommande året (eller den period man väljer att jobba med). För den som avser att helt efterleva 27001 är detta också ett uttalat krav – det ska finnas en aktuell internrevisionsplan gällande ledningssystemet för informationssäkerhet.

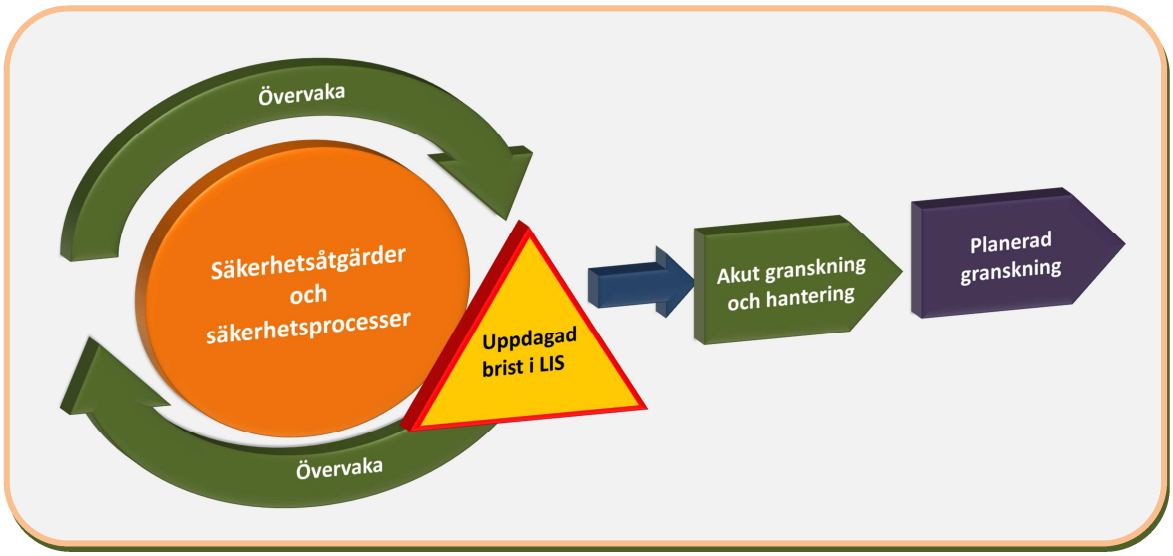
Planeringens utformning ska styras av verksamhetens behov, men ofta räcker det med några sidor som beskriver minst följande:

- **Period**: Vilken period avser planen (ex. 2016)
- **Inriktning**: Vad ska inriktningen på planerad granskning vara under perioden? (ex. ”granskning av kraven i avsnitt 4-8 i 27001”, eller ”granskning av säkerhetsåtgärdernas effektivitet och verkan”)
- **Metod**: Vilken metod ska användas (ex. visst verktyg, checklista eller metod)

## 3.2 Oplanerade granskningar

Ofta hinner man inte med att granska allt utan måste prioritera, och ledningen har då det yttersta ansvaret för prioriteringen. Det är också viktigt att planera för ”oförutsedda” granskningar. Övervakningen i den förra aktiviteten kommer troligen att visa ett antal tveksamheter i ledningssystemet. När dessa brister har åtgärdats akut mer djuplodande granskningar planeras.

**Figur 1.** Övervakning som visar på ett granskningsbehov



Aktiviteten Övervaka håller koll på att säkerhetsåtgärder och säkerhetsprocesser fungerar. Om en brist uppdagas hanteras den omedelbart och därefter kan man planera för en djupare analys av det inträffade.

# 4. Roller, metod och utmaningar

## 4.1 Ansvar och roller

### Ledningens ansvar

Enligt kraven i ISO 27001 ska ledningen

- Se till att interna revisioner av LIS genomförs
- Själva granska LIS genom ledningens genomgång
- Avsätta tillräckliga resurser för att genomföra granskningar
- Ta hand om resultatet av granskningarna.

### Ansvar för praktisk granskning

Många organisationer har en särskild funktion för internrevisioner som ska genomföra oberoende granskningar, oftast när det gäller ekonomi. Internrevisionen kan också ansvara för att granska verksamhetens förmåga att nå upp till sina mål och arbeta effektivt i övrigt.

Ledningssystemet och dess säkerhetsåtgärder kan mycket väl granskas av internrevisionen. Det viktiga är att granskarna inte är beroende av det de ska granska, för på så sätt kan granskningen bli objektiv och rättvisande.

### Kompetens för granskning

Granskarna behöver besitta kompetens på området de ska granska. Det kan gälla flera olika kompetenser eftersom informationssäkerhet innefattar många olika områden. Den som ska granska regelefterlevnad behöver till exempel juridisk kompetens, och det är nödvändigt med specifik teknisk kompetens när det gäller granskning av tekniska säkerhetsåtgärder.

## 4.2 Granskningsmetod

Hur själva granskningen genomförs beror på vad det är man ska granska.

**Granskning av säkerhetsåtgärder**
Återkommande granskningar av ”allmäntillståndet” kan man alltså göra genom att återanvända gapanalysen i processteget grundläggande analyser. Dokumentet Gapanalys med bilagor innehåller en utförlig metodbeskrivning av hur man gör en sådan granskning. Analysen kan dock behöva anpassas då och då så att den täcker nya säkerhetsåtgärder som organisationen har infört. Frågorna i den återkommande gapanalysen bör anpassas efter organisationens beslut om säkerhetsåtgärder.

**Granskning av ledningssystemet**
För granskning av ledningssystemets formella delar, och att de lever upp till kraven i 27001, utgår man från avsnitt 4-8 i standarden 27001. Det blir en bra granskningsmetod där man genom att gå igenom punkt för punkt säkerställer nuläget och eventuella förbättringsmöjligheter eller brister.

**Djupare granskningar**
Mer djupgående granskningar kan se olika ut beroende på vad som ska granskas, men oftast börjar man med att samla information om det som ska granskas. Informationen kan komma från olika källor och det kan gälla skriven information, i pappersform eller digitalt, eller muntlig information genom intervjuer eller gruppdiskussioner. Tidigare granskningar bör vara dokumenterade och blir då ett viktigt underlag för den nya granskningen. En annan viktig informationskälla är resultatet från övervakningen av informationssäkerheten (se dokumentet Övervakning).

## 4.3 Utmaningar

Det kan vara en delikat uppgift att utföra granskningar och den ansvariga granskaren måste förklara att granskningen är hjälp till självhjälp och inte handlar om att hitta syndabockar. Syftet med granskningen är att förbättra den granskade verksamheten och därmed säkerheten.

De som ansvarar för eller driver verksamheten som granskas kan dock lätt hamna i försvarsställning och försöka dölja eventuella brister. Därför är det viktigt att granskarna tidigt bygger bra relationer med resten av organisationen och har en positiv attityd till sin uppgift.

För att göra ett bra jobb måste granskarna också vara oberoende av den aktuella verksamheten och de berörda personerna.

Ytterligare en viktig förutsättning är att den granskade vet att den som granskar har mandat för detta och ledningens stöd.

# 5. Nästa steg

Resultatet av granskningen fungerar som en grund för ledningens genomgång, vilket är nästa steg. De granskningar som genomförts under tiden från föregående ledningens genomgång är en viktig källa till beslutsunderlag.