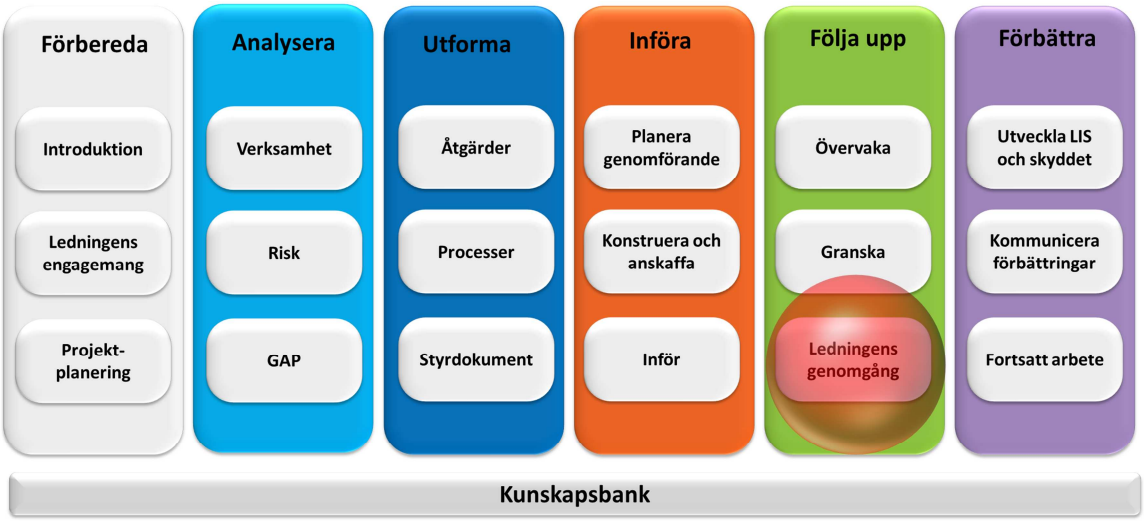
Myndigheten för samhällsskydd och beredskap

# Ledningens genomgång




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

Riskmiljön i verksamheten förändras hela tiden och detta gör att ledningen regelbundet måste få en helhetsbild när det gäller informationssäkerheten; vilka nya utmaningar ställs verksamheten inför och vilka beslut måste ledningen ta ställning till. Det kan tex vara förändringar i infrastrukturen, nya hot och säkerhetsrisker eller nya regulatoriska krav.

År 2006 och 2007 granskade Riksrevisionen elva myndigheter för att analysera deras styrning av informationssäkerheten. Analyserna visar att myndigheterna har problem med sin styrning. Så här sammanfattas de viktigaste ledningsproblemen:

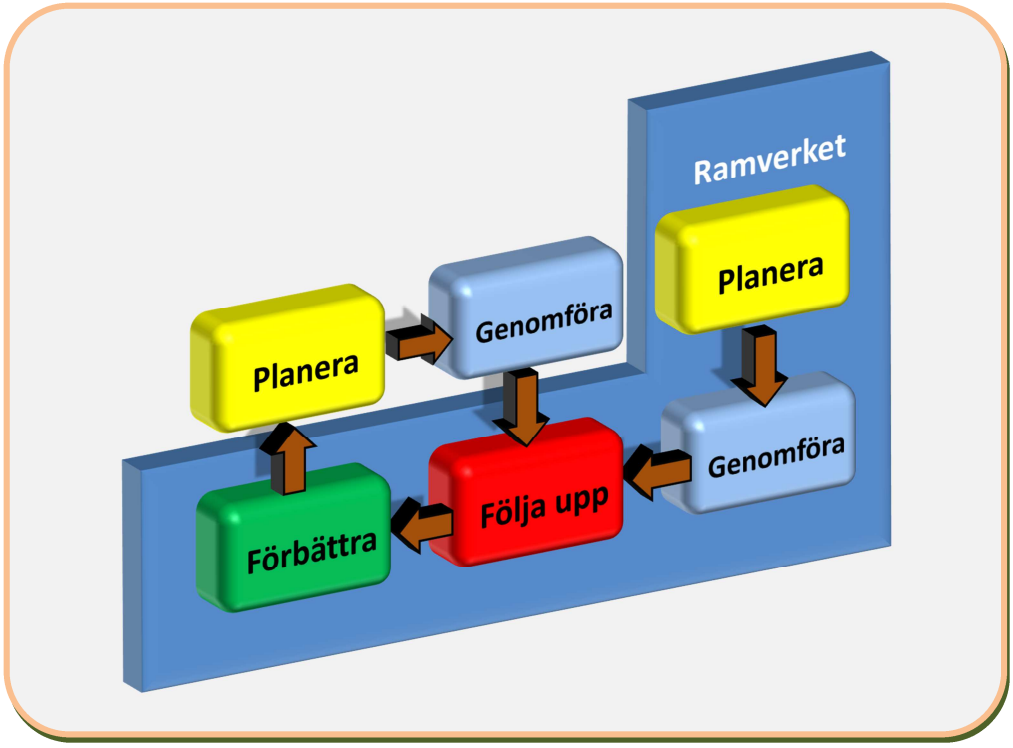
- Ledningen är osäker på vilka uppgifter den har i informationssäkerhetsarbetet och hur dessa uppgifter ska utföras.
- Ledningen begär inte något tydligt underlag om vilka risker och hot som finns för verksamheten. Ledningen får därmed inte tillräcklig insikt i vilka åtgärder som ska prioriteras för att skydda verksamheten.
- Ledningens beslut om säkerhetsåtgärder fullföljs inte.
- Ledningen följer inte upp om säkerheten uppfyller ledningens krav.
- Ledningen underrättar sig inte om att viktiga åtgärder som kontinuitetsplaner, rapportering och hantering av incidenter är utförda och fungerar som det är tänkt.
- Ledningen underskattar betydelsen av utbildning och information till personalen inklusive sin ledningspersonal och styrelsen.

Den här kritiken mot myndigheter kan gälla vilken verksamhet som helst. Därför är det viktigt att systematisera kontakten med ledningen så att de har en bra översikt över informationssäkerheten i verksamheten, och då är ledningens genomgång ett bra sätt.

## 1.1 Var vi är i processen

Metodstödet beskriver den första loopen i PDCA cykeln. När ledningen gör sin första genomgång kan det ändå hända att alla de beslutade säkerhetsåtgärderna och säkerhetsprocesserna ändå inte är på plats. Det gör dock inte så mycket eftersom det viktiga är att få igång processen för ledningens genomgång.

**Figur 1**: Första gången i PDCA -cykeln




## 1.2 Allmänt om ledningens genomgång

Enligt standarden ISO 27001 är ett LIS den del av det *övergripande* ledningssystemet som ska upprätta, införa, driva, övervaka, granska, underhålla och förbättra informationssäkerheten. Ledningens genomgång ska präglas av att verksamheten har ett ledningssystem och att faktiska säkerhetsåtgärder införs. Syftet är att verksamheten ska ha rätt säkerhet utifrån de risker och krav (legala krav och avtalskrav) som finns.

MSB skriver i sina föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2009:10) att myndighetsledningar ska hålla sig informerade om arbetet med informationssäkerhet. Denna föreskrift ger information om att ledningen löpande ska hålla sig informerad om vad som händer, och att det lämpligast sker genom att man i den ordinarie avrapporteringen för verksamhetsplaneringen även avrapporterar informationssäkerheten.

Genomgången ska innefatta bedömningar av möjligheter till förbättring och behovet av förändringar i ledningssystemet, inklusive policy och mål för informationssäkerheten. Resultaten från ledningens genomgång ska tydligt dokumenteras och dokumenten ska bevaras
Åtgärden syftar även till att ledningen på strategisk nivå ska få kunskap om ”informationssäkerhetsläget”.

## 1.3 Roller

Följande roller bör medverka i att ta fram underlaget för ledningens genomgång:

- den informationssäkerhetsansvariga
- ansvariga för de olika delarna i standarden 27002.

## 1.4 När ska ledningens genomgång genomföras?

Ledningen bör gå igenom informationssäkerheten ungefär samtidigt som den går igenom de övriga ledningssystemen. Det är viktigt att samordna arbetet så att resultatet kan införas i den planeringsprocess verksamheten har.

## 1.5 Underlag för genomgång

Underlaget för ledningens genomgång inkluderar:

- information om resultat av revisioner och granskningar av informationssäkerheten
- återkoppling från intressenter, tekniker, produkter eller rutiner som skulle kunna användas för att förbättra prestanda och verkan på informationssäkerheten
- sårbarheter, hot och alla förändringar som kan påverka informationssäkerheten
- rekommendationer till förbättringar

## 1.6 Resultat av genomgång

Resultaten från ledningens genomgång ska innefatta beslut och åtgärder som rör förbättring av verkan av informationssäkerheten, nödvändiga anpassningar av rutiner och säkerhetsåtgärder som påverkar informationssäkerheten och förbättring av sättet att mäta dess verkan.

## 1.7 Ett verksamhetssystem

Om verksamheten har flera ledningssystem (som tillsammans bildar ett verksamhetssystem) bör det finnas en gemensam process för att ta fram underlag till verksamhetssystemet, och denna process bör gälla även för ledningens genomgång. I detta dokument visas ett exempel på kopplingen mellan kvalitetssystemet, miljösystemet, arbetsmiljösystemet och informationssäkerhetssystemet.

Dokumentet Utforma LIS beskriver de processer som behövs för informationssäkerhetsområdet, med ett *processkort* för ledningens genomgång. Bilaga A innehåller ett exempel på ett sådant kort som anger de olika delar som ska ingå i genomgången.

# 2 Att genomföra ledningens genomgång

Ledningen behöver ett strukturerat beslutsunderlag för att kunna avgöra om alla säkerhetsåtgärder och ledningssystem uppfyller kraven. Detta underlag bygger på de säkerhetsåtgärder och säkerhetsprocesser som satts upp, och en viktig informationskälla är underlagen från stegen *övervaka* och *granska*.

Standarden 27001 anger hur beslutsunderlaget bör vara uppbyggt. Beskrivningen i det här dokumentet frångår dock standarden något för att få en rubrikindelning i rapporten som stämmer med de andra ledningssystemen.

Underlagsrapporten kan då bestå av följande avsnitt:

1. Introduktion
2. Uppföljning av tidigare beslut
3. Resultat från tidigare revisioner (interna och externa) och andra granskningar
4. Status när det gäller förebyggande och korrigerande åtgärder (inklusive sårbarheter och hot mot LIS)
5. Inkomna reaktioner från kunder och intressenter (inklusive klagomål)
6. Resultat av mätningar inklusive process- och miljöprestanda
7. Överensstämmelse med krav och mål
8. Utvärdering av lagefterlevnad
9. Förändrade förhållande som kan påverka ledningssystemet
10. Rekommendation till förbättringar
11. Förkortningar
12. Referenser
13. Dokumentets revisionshistoria

## 2.1 Planera och förbereda ledningens genomgång

Det första steget är att planera arbetet med att ta fram en rapport och att boka in ett möte för ledningens genomgång. Det går att samordna ledningens genomgång med de andra ledningssystemen i verksamheten, och då måste arbetet samordnas med de personer som ansvarar för de ledningssystemen.

Underlaget till rapporten bör till största delen komma från stegen övervaka och granska. Den information som ska ingå är

- resultat av revisioner och granskningar av LIS
- återkoppling från intressenter
- tekniker, produkter eller rutiner som skulle kunna användas i organisationen för att förbättra LIS prestanda och effekt
- status när det gäller förebyggande och korrigerande säkerhetsåtgärder
- sårbarheter eller hot som inte behandlades tillräckligt vid den föregående riskbedömningen
- mätresultat som visar effekten av ledningssystemet och säkerhetsåtgärderna
- uppföljning av aktiviteter från ledningens tidigare genomgångar
- alla förändringar som kan påverka LIS
- en analys av inträffade incidenter
- rekommendationer till förbättringar.

Om underlaget inte är tillräckligt kan man behöva göra egna kontroller och ta fram de underlag som krävs. Det bör även göras en bedömning om det finns några externa tjänster eller parter som ska granskas.

När informationen ovan har kommit in ska den skrivas in i rapporten på rätt plats. Den kompletta rapporten ska sedan sändas ut på remiss till de nyckelpersoner som har en uppgift i ledningssystemet samt de chefer som berörs. Ibland kan det även vara lämpligt att först sända rapporten till fackliga representanter för synpunkter. Målet är att innehållet ska vara väl förankrat när ledningen till sist får rapporten.

I planeringen ingår att boka ett rum för ledningens genomgång. Välj ett välbekant rum med teknik som passar för genomgången. Mötet kan ta en eller två timmar beroende på upplägget. Om ledningen förväntas besluta om förbättringsåtgärder för ledningssystemet kan det behövas två timmar så deltagarna får tid att diskutera. Beroende på organisationen kan det vara lämpligt att boka in tiden för ledningens genomgång ett kvartal i förväg, för att vara säker på att få tillräckligt med tid. Försök också att få in mötet i den kalender som varje verksamhet brukar ha för sin planeringsprocess. Tiden bör anpassas så att eventuella förbättringsförslag kommer med i nästa års verksamhetsplan.

När rapporten är klar är det dags att skapa presentationen inför mötet. Provkör presentationen för att se hur lång tid genomgången kan ta.

Rapporten bör sändas ut till ledningen minst en vecka före mötet. De bilder som hör till materialet kan skickas ut före eller delas ut på mötet.

## 2.2 Genomföra ledningens genomgång

Det går att inkludera flera ledningssystem i samma genomgång (genomgång av verksamhetssystemet). Då är det lämpligt att utse en person som håller i presentationen medan de andra är redo att svara på mer specifika frågor .

Var tydlig med vilka beslut ledningen bör fatta på plats under mötet. Om en fråga bordläggs kan det dröja länga innan ledningen samlas nästa gång.

Var konkret vid presentationen. Beskriv förslaget klart och tydligt och ge ett tydligt exempel på konsekvenserna. Undvik tekniska detaljer utan fokusera på effekten om förslaget blir verklighet. Kom ihåg att ha väl underbyggda och dokumenterade motiveringar till varje förslag.

## 2.3 Följa upp ledningens genomgång

Efter mötet är det dags att ta tag i resultatet som bör innefatta beslut och åtgärder som rör

- förbättring av LIS effekt
- uppdatering av riskbedömnings- och riskbehandlingsplanen
- nödvändiga anpassningar av rutiner och säkerhetsåtgärder som påverkar informationssäkerheten, med ändringar av
    - verksamhetskrav
    - säkerhetskrav
    - verksamhetsprocesser som påverkar de gällande verksamhetskraven
    - författningskrav
    - åtaganden i avtal
    - risknivåer och/eller kriterier för riskacceptans
    - resursbehov
- förbättring av sättet att mäta säkerhetsåtgärdernas effekt

## 2.4 Förbättra ledningssystemet

Sedan är det dags att förbättra ledningssystemet genom att införa de beslutade åtgärderna eller ändra någon inriktning i verksamhetsstyrningen.. Ofta är det saker som kan göras direkt. De lite större och systematiska felen måste införas i verksamhetsplanen för nästa år.

Förbättringsåtgärderna kan grupperas inom områdena

- ledning och organisation
- procedurer (till exempel backup och incidenthantering)
- processer (till exempel riskhantering)
- teknik (till exempel accesskontroll)
- fysiska åtgärder (till exempel tillträde och brandskydd).

# 3 Nästa steg

Ledningen har nu kontrollerat om arbetet med informationssäkerhet stämmer överens med kraven och bestämt vilka brister som måste åtgärdas. Nästa steg handlar om arbetet med att förbättra ledningssystemet och höja informationssäkerheten.

# Bilaga A: Exempel på processkort för ledningens genomgång av informationssäkerheten

| | | |
|---|---|---|
| **Processnamn** | | Ledningens genomgång av informationssäkerheten |
| **Allmän beskrivning** | | Under verksamhetens fortlöpande arbete ska ledningen kontrollera planer och fastställda mål. Detta kräver en genomgång av informationssäkerheten. |
| **Syfte** | | Syftet är att ledningen på strategisk nivå ska få kunskap om informationssäkerhetsläget och fatta beslut om förändringar och förbättringar av säkerhetsåtgärder samt se över policy och mål för informationssäkerheten |
| **Mål** | | Målet är att besluta om eventuella insatser och förändringsåtgärder som behövs för att nå målen. |
| **Indata** | | Alla underlag som beskriver statusen på informationssäkerheten. Tex revisioner, incidentrapporter och mätdata. |
| **Utdata** | | Beslutade förändringar och förbättringar inom detta och nästa verksamhetsår. |
| **Arbetsresultat** | | Beslut och handlingsplan för förbättrings- och förändringsåtgärder inom verksamhetsåret och för den kommande verksamhetsplaneringen. |
| | |  |
| **1** | **Planera och förbereda ledningens genomgång** | a) Samla ihop underlag<br>b) Skriv rapport<br>c) Boka in mötestid med ledningen<br>d) Ta fram presentation |
| **2** | **Genomföra ledningens genomgång** | a) Genomför ledningens genomgång |
| **3** | **Följa upp ledningens genomgång** | a) Utvärdera resultatet av ledningens genomgång<br>b) Utvärdera mötet ledningens genomgång<br>c) Ta fram eventuell handlingsplan<br>d) Uppdatera eventuellt dokumentation |

| | | |
|---|---|---|
| **4** | **Förbättra ledningssystemet** | a) Inför förbättringar som ryms inom verksamhetsåret<br>b) Ta fram underlag till nästa verksamhetsplanering |
| **Intressenter** | | Hela verksamheten, alla myndigheter, alla chefer och alla anställda |
| **Information** | | Verksamhetsplanen, verksamhetspolicyn, riktlinjer för informationssäkerhet, IT-säkerhetspolicy, riktlinjer för IT-säkerhet etc. |
| **Stöd** | | Intranätet, utbildningsenheten, säkerhetsansvariga etc. |
| **Övrigt** | | |

# Bilaga B - Exempel på instruktion för ledningens genomgång

Denna bilaga är ett exempel på en instruktion för ledningen genomgång.

## 1. SYFTE

Syftet är att beskriva ledningens genomgång av verksamhetssystemet (ledningssystem för kvalitet, miljö och informationssäkerhet samt systematiskt arbetsmiljöarbete) (ref. 1).

## 2. INNEHÅLL

### 2.1 ALLMÄNT

Högsta ledningen på X-myndigheten går en gång per år (i februari) igenom verksamhetssystemet för att kontrollera att systemet är lämpligt, tillräckligt och effektivt. Genomgången ska innefatta en bedömning av möjligheterna att förbättra och behovet av att ändra ledningssystemen, inklusive policy och mål. En sammanställning av kraven i respektive standard när det gäller underlaget för ledningens genomgång visar om det går att ha en integrerad rapportering (ref. 2, 3, 4, 5, 6).

Planeringsdirektören är ansvarig för ledningens genomgång och kvalitetschefen förbereder genomgången med en gemensam rapport till ledningen (ref. 7). Varje funktion ska ta fram en rapport (ref. 8) för sitt område, dvs. den som är ansvarig för kvalitet ska rapportera kvalitetsdelen, den miljöansvarige ska rapportera miljödelen, säkerhetschefen ska rapportera informationssäkerhetsdelen och HR-chefen ska ta fram underlag som rör arbetsmiljöarbetet. Underlaget ska skickas till den kvalitetsansvarige personen senast 3 veckor innan ledningen har sin genomgång. Den kvalitetsansvarige ska se till att rapporten i sin helhet kvalitetssäkras innan den lämnas till och redovisas för ledningsgruppen.

Genomgången dokumenteras med ett protokoll. Som bilaga ska det finnas en handlingsplan med uppgifter om vem som ansvarar för de beslutade korrigerande åtgärderna samt när åtgärderna bör vara klara. Underlagen, rapporten, protokollen och handlingsplanen arkiveras i dokumenthanteringssystemet.

# 3. UNDERLAG FÖR GENOMGÅNG

## 3.1 KVALITET, MILJÖ OCH INFORMATIONSSÄKERHET

Underlaget för ledningens genomgång ska innefatta

- uppföljning av tidigare beslut
- resultat från revisioner (interna och externa) och andra granskningar
- status när det gäller förebyggande och korrigerande åtgärder (inklusive sårbarheter eller hot mot LIS)
- reaktioner från kunder och intressenter (inklusive klagomål)
- mätresultat som visar effekten , inklusive process- och miljöprestanda
- överensstämmelse med krav och mål
- utvärdering av lagefterlevnad
- förändrade förhållanden som kan påverka ledningssystemen
- rekommendationer till förbättringar.

## 3.2 ARBETSMILJÖ

Underlaget som gäller det systematiska arbetsmiljöarbetet ska så långt det är möjligt motsvara underlaget för kvalitets-, miljö- och informationssäkerhetsområdet.

# 4. RESULTAT AV GENOMGÅNG

Ledningens genomgång ska resultera i beslut och åtgärder som rör

- förbättring av verksamhetssystemets och dess processers effekt
- anpassning till kunders och intressenters krav
- behov av resurser.

# FÖRKORTNINGAR OCH DEFINITIONER

| | |
|---|---|
| LIS | Ledningssystem för informationssäkerhet |

# REFERENSER

1. Verksamhetsmanualen
2. Ledningssystem för kvalitet – Krav, SS-EN ISO 9001:2008 kap. 5.6
3. Miljöledningssystem – Krav och vägledning, SS-EN ISO 14001:2004 kap. 4.6
4. Ledningssystem för Informationssäkerhet – Krav, ISO/IEC 27001:2005
5. Instruktion för Systematiskt arbetsmiljöarbete
6. SS-EN ISO/IEC 17025:2005 Allmänna kompetenskrav för provnings- och kalibreringslaboratorier
7. Rapportmall. Sökväg: Word/Officeknappen/Nytt/Mina mallar/Kvalitetsdokument/ Ledningens genomgång
8. Rapportmall. Sökväg: Powerpoint/Officeknappen/Nytt/Mina mallar/xxx/Ledningens genomgång

# HISTORIK

| Datum | Version | Orsak/författare |
|---|---|---|
| | 0-1 | Upprättat utkast till instruktion för ledningens genomgång./ XX-p |