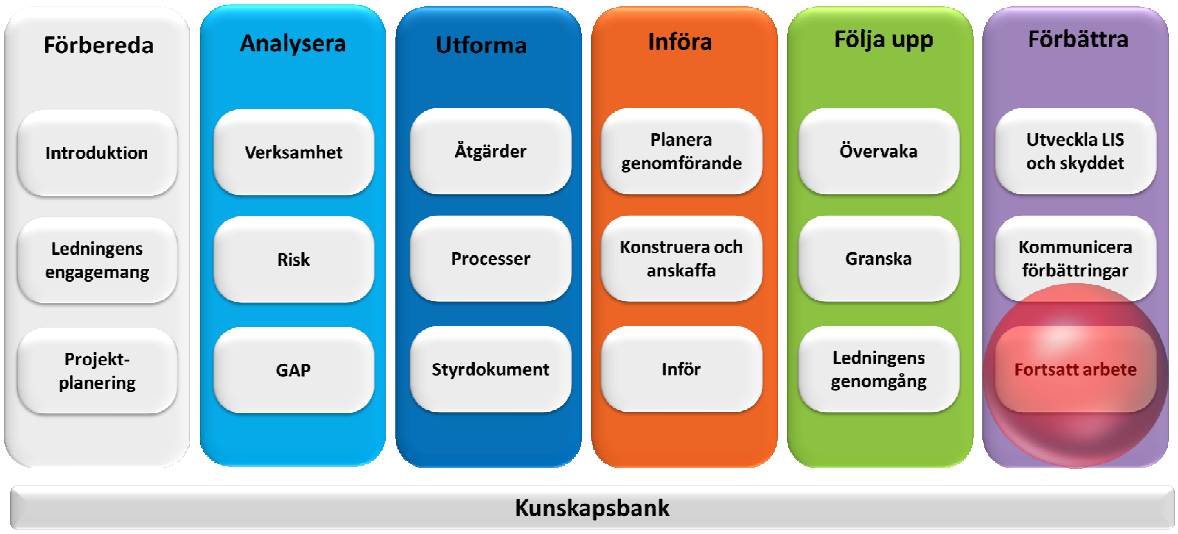
Myndigheten för samhällsskydd och beredskap

Fortsatt arbete



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 detta dokument är att beskriva hur vi går från projektet där vi haft syfte att införa ett ledningssystem och dess säkerhetsåtgärder och säkerhetsprocesser till att i vardagen tillämpa det vi infört. LIS projektet har genom sitt arbete:

1. Tagit fram verksamhetens behov.
2. Utifrån behovet infört säkerhetsåtgärder och processer i allmänhet och speciellt de processer som behövs för styrningen som övervakning, granskning, ledningens genomgång och hur vi utvecklar skyddet.
3. Tagit fram styrande och stödjande dokument.
4. Tagit fram den styrprocess som måste finnas för att vi ska strategiskt ska kunna styra informationssäkerhetsarbetet och göra ledningen delaktig.

Nu är ledningssystemet infört och funktionaliteten har verifierats under en längre tid. Ledningssystemet har blivit en integrerad del av verksamheten. De grundläggande principerna för det fortsatta informationssäkerhetsarbetet är:

- **Informationssäkerhet skapar ett värde för verksamheten.**
  Säkerhet skapar en möjlighet för verksamheten att nå sina mål på ett effektivt sätt och bidrar till trygghet och säkerhet för personalen och till att verksamheten följer lagar och regelverk. Allt detta gör även att verksamhetens förtroende ökar.
- **Informationssäkerhet är integrerat i verksamhetens alla processer.**
  I allt man gör i verksamheten ska man ta hänsyn till de risker som kan uppkomma och göra bedömning om hur de ska hanteras. Detta ska även göras i projekt.
- **Informationssäkerhet och riskhantering är en del av verksamhetens beslutsprocess.**
  Att tänka i risker gör att alla beslut som fattas i verksamheten blir väl balanserade och man får ett medvetet risktagande.
- **Säkerhetsbedömningar är att hantera det okända.**
  Att vi arbetar med säkerhet gör att vi ställer oss frågan; om vi gör detta, vad får det för konsekvenser? Vi tänker i OM-fall vilket gör att vi kan ställa olika delar mot varandra och därigenom får bättre beslut och handlande.
- **Informationssäkerhetsarbetet skapar struktur, systematik och tidsstyrning.**

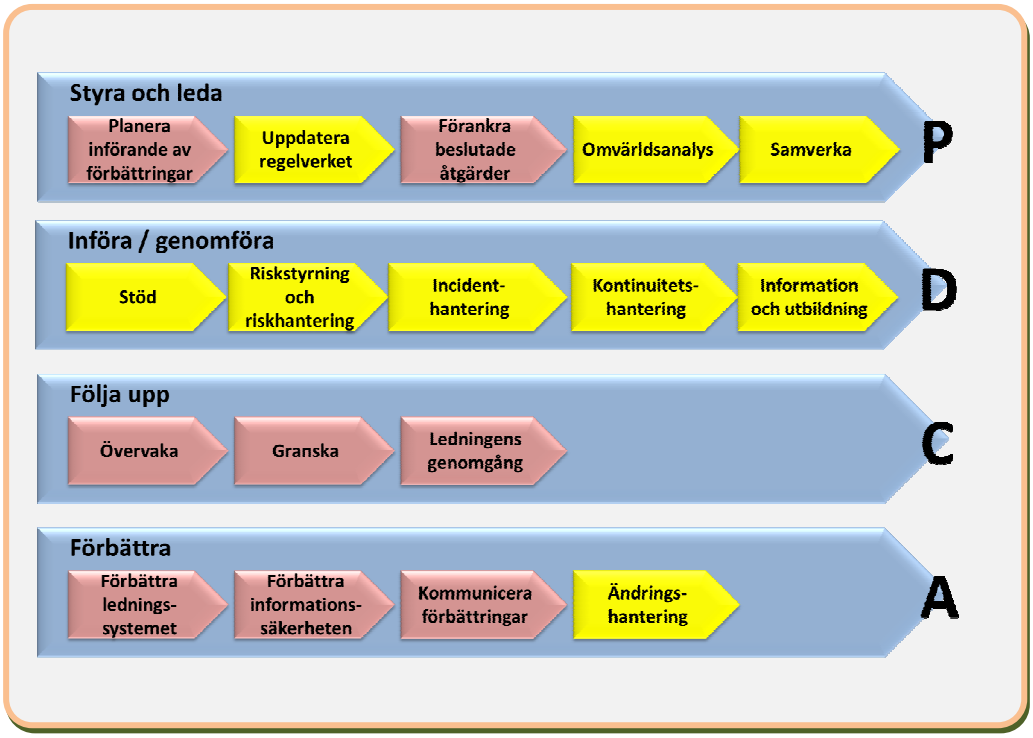
Arbetar vi på rätt sätt med P-D-C-A med säkerhet som en process får vi ett effektivt sätt att genomföra vår verksamhet.

- **Informationssäkerhetsarbetet kan skräddarsys utifrån verksamhetens behov.**
  Verksamhetens mål, krav, kultur och risksituation styr vilken nivå på säkerheten verksamheten ska ha.

- **Vi arbetar med ständig förbättring.**
  Arbetar vi strukturerat med ett ledningssystem får vi en process för ständig förbättring.

De processer som byggdes upp i LIS införandet ska underlätta arbetet med dessa frågor i vardagen. Bilden i figur 1 är ett exempel från processteget att *utforma LIS*. Den visar en övergripande karta över de processer som kan behövas inom informationssäkerhetsarbetet. Kartan beskriver både processer som stöttar själva LIS-arbetet (de röda pilarna) och operativa säkerhetsprocesser för att införa och genomföra (de gula pilarna).

Figur 1. Operativa och strategiska processer



2. Framgångsfaktorer

Det finns flera framgångsfaktorer som leder till ett lyckat fortsatt arbete. Några viktiga faktorer är:

- Att stödja verksamheten i informationssäkerhetsfrågor och riskhantering.
- Att styra vårt område och i denna styrning vara offensiva och sätta mål för vad som ska uppnås.
- Att följa upp, utvärdera och utöva tillsyn av vårt område.
- Att ta fram relevanta, tydliga och tillförlitliga beslutsunderlag till ledningen så att de fattar medvetna riskbeslut.
- Metodutvecklingen inom informationssäkerhetsområdet ska vara inriktad mot framsteg och resultat.
- Genomför samordnade aktiviteter och ha enhetliga budskap.
- Varje medarbetares engagemang och kompetens ska tas tillvara.
- Ha ett effektivt resursutnyttjande och hög leveransförmåga.
- Vi ska ha koll på vad som händer i verksamheten.
- Skapa former för samverkan med andra för att få information och tips om hur andra gör.
- Ge ledningen löpande en korrekt bild av informationssäkerheten.
- Ta små steg genom ständig förbättring.

Det är också viktigt att jobba vidare med de delar som inte hanterades i LIS-projektets första fas. När ett projekt genomförs görs alltid avgränsningar och under projektets gång kommer det alltid upp saker som borde ingå i projektet men inte hinns med. Analysera dessa och skapa en strategi för hur dessa övertiden ska hanteras.

3. Det praktiska vardagliga arbetet

För att säkra en fortsatt hög nivå på informationssäkerheten är det viktigt att tänka på bland annat att:

- Alla som arbetar inom eller har uppdrag åt organisationen ska känna trygghet och ges stöd vid hot, angrepp och andra incidenter.
- Information värderas, skyddas och finns tillgänglig när den behövs.
- Utrustning hanteras och förvaras på ett säkert sätt.
- Lokaler utformas och skyddas för att säkerställa verksamheten.

För att detta ska fungera bör informationssäkerhetsarbetet ha följande förmågor:

- **Att strategisk styra, leda, följa upp och utveckla informationssäkerhetsarbetet.** Informationssäkerhetsfunktionen ska som verksamhetens strategiska säkerhetsorgan vara omvärldsorienterad och utveckla och stödja informationssäkerheten.
- **Arbeta riskstyrt.** Verksamheten ska ha rätt säkerhet utifrån verksamhetens krav och risker.
- **Informera och utbilda.** Det handlar om att ge tillräckligt med kunskap och information för att skapa förståelse för åtgärderna hos medarbetarna, påverka deras riskbeteende och övergå till säkrare sätt att handla.
- **Samverka.** En förutsättning för engagemang är delaktighet vilken skapar förståelse för informationssäkerhetsarbetets mål, behov och förutsättningar.
- **Följa upp.** I en väl fungerande styrning läggs lika mycket kraft på uppföljning som på planering.

Det praktiska vardagliga informationssäkerhetsarbetet kan delas in i de arbetsuppgifter som syftar till att leda och styra själva informationssäkerhetsfunktionen, och de arbetsuppgifter som andra gör inom verksamheten. Om informationssäkerhetsarbetet är en integrerad del i en säkerhetsfunktion kan denna modell användas för hela säkerhetsarbetet. Detta

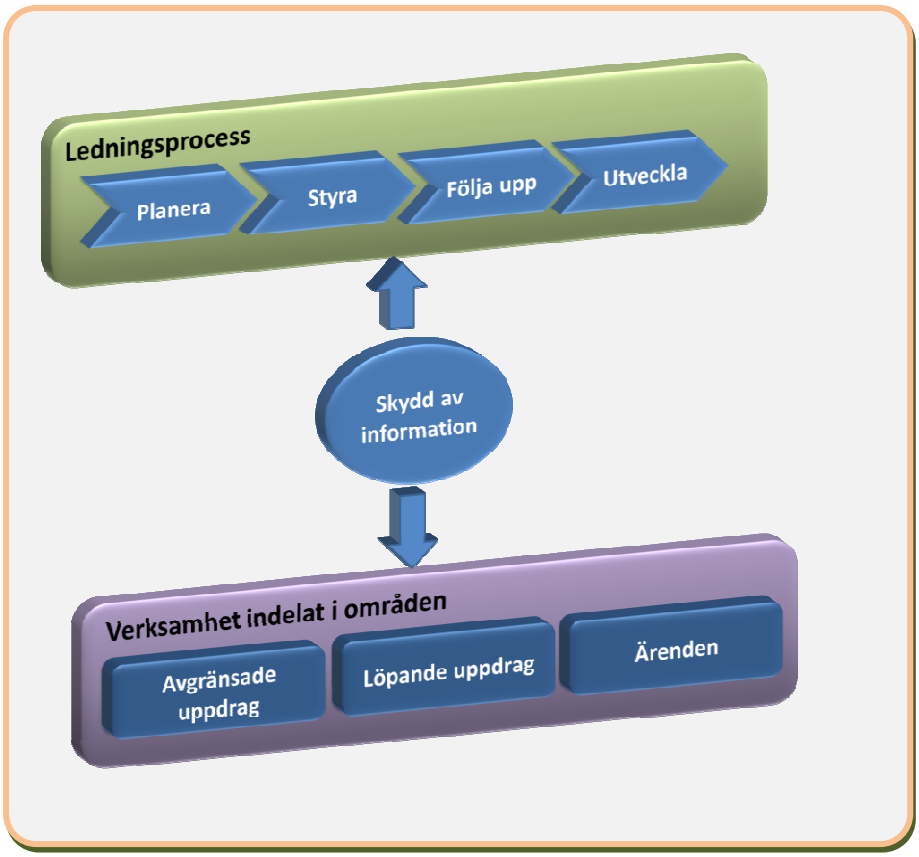
kallar vi för Ledningsprocessen och illustreras i figur 2. Som framgår av bilden gör organisationen följande:

- Planerar
- Styr
- Följer upp
- Utvecklar vårt arbete inom informationssäkerhetsområdet

För att kunna hantera de uppgifter och allt som faller på en informationssäkerhetsfunktion måste arbetet delas upp i olika *arbetsområden* för att kunna få bra styrning på verksamheten. En lämplig indelning, som diskuteras mer ingående i avsnitt 5 är:

- **Avgränsade uppdrag**
    - Planeras genom ledningsprocess
    - Avgränsade, ej återkommande uppdrag med start och slut
    - Initieras endast genom beslut i ledningsprocess
    - Arbetet utgörs i uppdrag/projektform
- **Löpande uppdrag**
    - Planeras genom ledningsprocess
    - Löpande uppdrag (linje), inget slutdatum
    - Initieras endast genom beslut i ledningsprocess
    - Arbetet utförs både i process – och uppdrags/projektform
- **Ärenden**
    - Planeras schablonmässigt genom ledningsprocess
    - Kort genomförandetid för respektive ärende
    - Initiering av arbetet (enskilt arbete) är händelsestyrt
    - Arbetet utförs i processform

Figur 2. Det vardagliga informationssäkerhetsarbetet



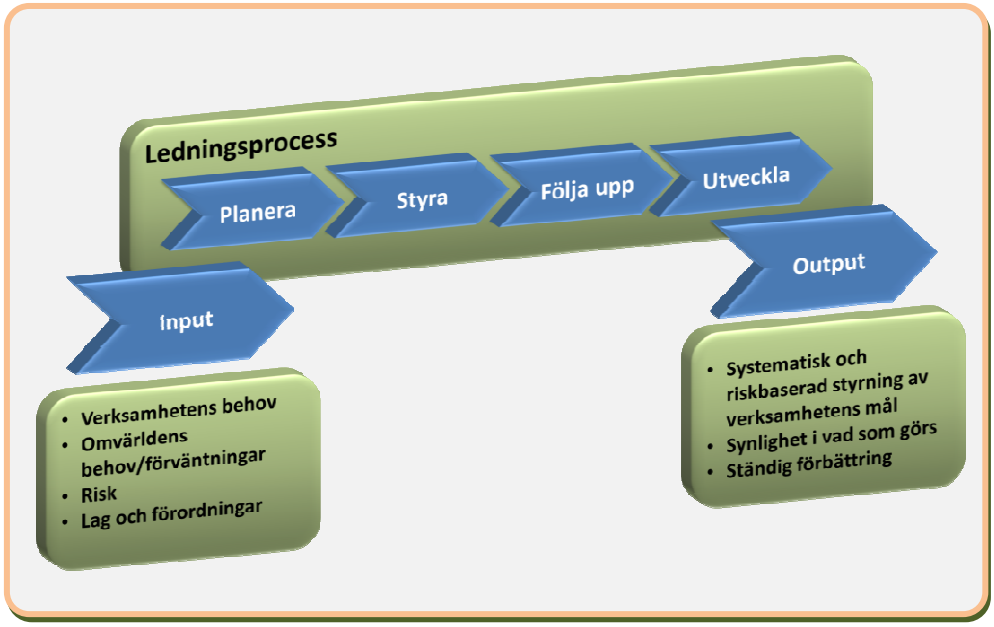
Det räcker dock inte med ovanstående beskrivning för att förstå vad som görs i mer detalj. I nästa stycke diskuteras därför de olika stegen i *ledningsprocessen*.

4. Ledningsprocessen

Ledningsprocessen består av fyra områden:

- Planera
- Styra
- Följa upp
- Utveckla

Figur 3. Beskrivning av ledningsprocessen



Ledningsprocessen är ett ledningssystem för verksamhetsstyrning som bygger på PDCA. Säkerhetschefen eller informationssäkerhetschefen äger ledningsprocessen. Målet för ledningssystemet är att uppfylla uppdraget (målet) i informationssäkerhetspolicyn, på ett effektivt sätt.

Ett team av personer utför de olika delprocesserna i ledningsprocessen. I början görs endast en övergripande fördelning, till exempel där chefskap och befogenhet enligt arbetsordning har betydelse.

Ledningsprocessen tar ansvar för att alla uppgifter som utförs i verksamheten är korrekt fördelade och prioriterade.

4.1 Planera

Detta område består i verksamhetsplanering, resursplanering och omvärldsbevakning. För var och en av dessa ingår följande aktiviteter:

4.2 Styra

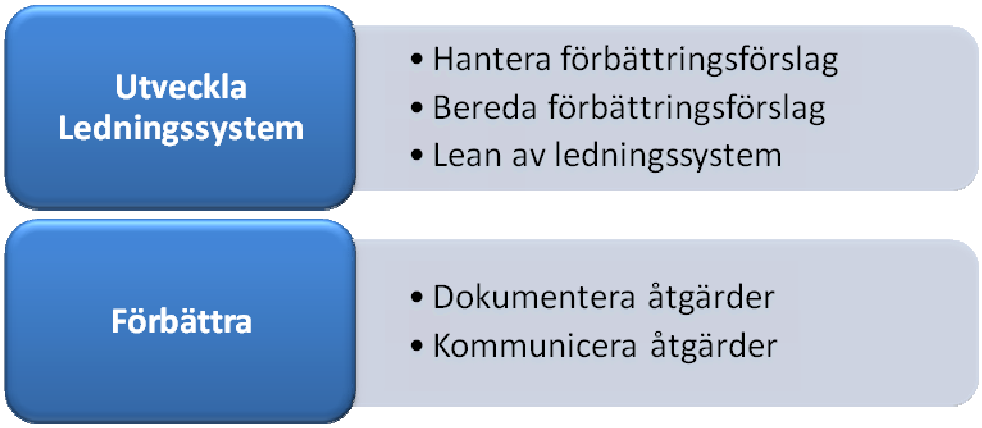
4.3 Följa upp

I den grå delen finner ni exempel på delar som bör följas upp. Under *ledning* ingår ledningens genomgång som bör genomföras minst en gång per år. Här

ska även de delar som görs som uppdrag, aktiviteter och ärenden plockas upp. Denna del gör att verksamheten kan visa vad som gjorts under året.

4.4 Utveckla

Det är inte alltid möjligt att ta de stora steg som önskas i informationssäkerhetsområdet. Istället måste man ofta ta små steg för att uppnå ständiga förbättringar. Även här finner ni flera aktiviteter under respektive process steg.



5. Arbetsområden för fortsatt arbete

Det nämndes tidigare att det fortsatta arbetet kan delas upp i tre arbetsområden - *avgränsade uppdrag, löpande uppdrag* och *ärenden*.

Arbetsområdena samlar alla uppgifter som görs för att uppfylla målen för informationssäkerhetsarbetet. De är uppdelade i tre (3) arbetsområden där uppgifter av olika ”typ” samlas områdesvis. Allt arbete organiseras delvis i en matrisorganisation med flera olika ansvarsroller, ansvarsområden och ämnesspecialister med särskilda uppdrag och enskilda befattningar. Uppgifterna utförs i olika arbetsformer utefter vad som är bäst lämpat för uppgiften, bl.a. process, uppdragsform samt projektform.

De avgränsade uppdragen består av aktiviteter vi gör inom följande områden:

- Verksamhetsutveckling
- Utbildning
- Kontroll
- Projektbeställning

Löpande uppdrag består av:

- Beställning av tjänster som informationssäkerhetsfunktionen köper från verksamheten eller av andra.
- Säkerhetsskydd
- Incidentstyrning
- Krisberedskap
- Ledningens genomgång
- Signalskydd
- Samverkan internt
- Samverkan externt
- Systemägarskap
- Information/kommunikation
- Strategisk utveckling av informationssäkerheten
- Förvaltning av styrande- och stödjandedokument

Området ärenden består av:

- Incidentutredning
- Remisser
- Yttrande / säkerhetsfrågor
- Analys- och utredningsstöd
- Granskning (ackreditering / godkännande)
- Granskning Övrigt
- Loggutdrag

6. Avslutning

Vi har velat visa hur ni kan arbeta vidare i en ständigt återkommande process med informationssäkerhetsområdet och självklart kan vi i vårt fortsatta arbete återanvända mycket av det vi tog fram och använde i LIS-projektet.