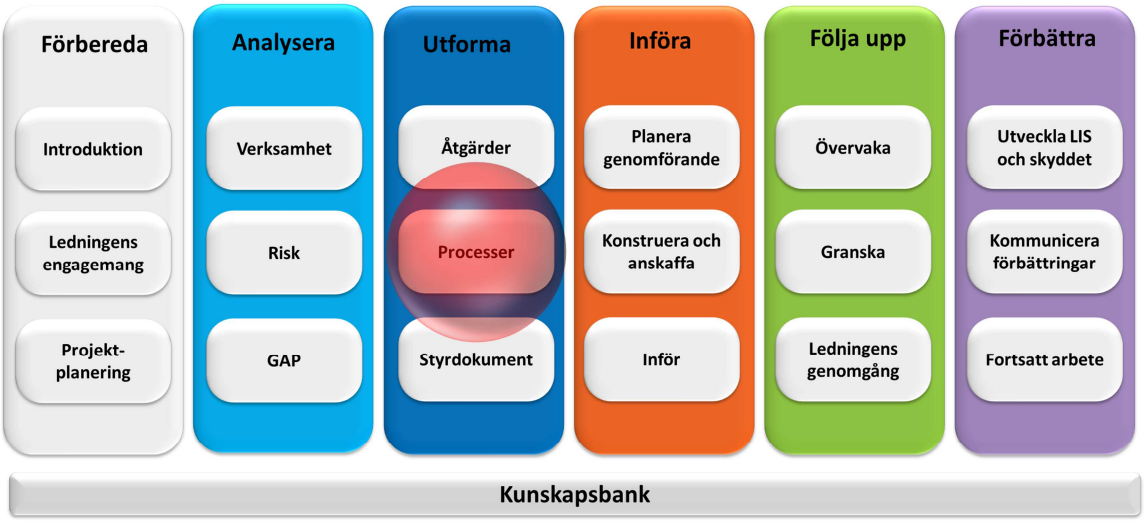
Myndigheten för samhällsskydd och beredskap

Utforma säkerhetsprocesser



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

De flesta säkerhetsåtgärder som införs i en verksamhet kräver systematiskt underhåll och ständig tillsyn. Det finns väldigt få säkerhetsåtgärder som kan införas en gång för alla och sedan fungera i all framtid. Ett virusskydd blir till exempel snabbt värdelöst om det inte uppdateras, och ett larmsystem blir opålitligt om behörighetsinformationen inte är aktuell. Det behövs alltså en eller flera *processer* för att vara säker på att en införd säkerhetsåtgärd fortsätter att fungera effektivt. I vissa fall är det faktiskt själva processen som *är* säkerhetsåtgärden. Exempelvis kan incidenthantering betraktas som en säkerhetsåtgärd som bygger på ett antal dokumenterade aktiviteter.

1.1 Säkerhetsprocesser

Med ”process” menas en samling förbestämda, länkade och dokumenterade aktiviteter som svarar mot ett fastställt behov. En ”säkerhetsprocess” gäller här en process som är renodlad för att hantera informationssäkerhet. Om det är möjligt ska man i stället sträva efter att *integrera* säkerhetsåtgärderna i processer som redan finns i verksamheten. En del verksamheter har dock inga väldefinierade processer att utgå ifrån, och då blir det ändå nödvändigt att utforma specifika säkerhetsprocesser. De processer som påverkar en större del av verksamheten eller som går längre än informationssäkerhetsbehovet som kontinuitetsprocessen kräver ofta mer från projektet.

Genom att tänka i processer skapas flöden som är viktiga för att informationssäkerhetsarbetet ska fungera effektivt. Processerna är också en viktig utgångspunkt för att regelbundet *granska* arbetet. Dessutom gör processerna det lättare att överblicka hur saker påverkar varandra eller är beroende av varandra samt hur de stöttar verksamhetens krav och mål för informationssäkerhetsarbetet. Att beskriva processer är att identifiera *vad* som måste göras, och *hur*, samtidigt som man tydligt *kommunicerar* vad som görs. En tydligt definierad process underlättar arbetet i nästa steg när det är dags att ta fram policy- och styrdokument.

1.2 Syfte

De säkerhetsåtgärder som ska införas (se ”Fastställa säkerhetsåtgärder”) påverkar och påverkas av ett antal processer i verksamheten. Syftet med att utforma säkerhetsprocesserna är att identifiera, kartlägga och uppdatera dessa verksamhetsprocesser.

Målet är att ta fram och dokumentera de nödvändiga säkerhetsprocesserna med de ingående aktiviteter och ansvariga personer.

1.3 Utforma säkerhetsprocesser

Aktiviteten ”fastställa säkerhetsåtgärder” gick ut på att dokumentera de tekniska eller administrativa säkerhetsåtgärder som ska införas. En del av dessa säkerhetsåtgärder består av, eller är beroende av, processer som måste finnas på plats för att skydda verksamhetens information.

För att utforma säkerhetsprocesser identifierar man först vilka processer som verksamheten behöver och kartlägger sedan de verksamhetsprocesser som redan finns. Eventuellt blir det nödvändigt att utforma nya processer.

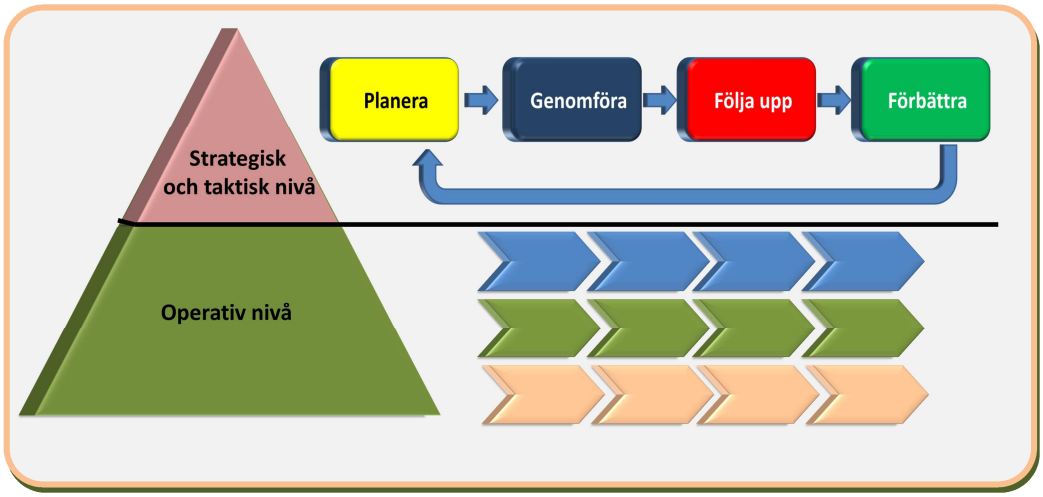
Arbetet omfattar dels de specifika säkerhetsprocesserna på operativ nivå, dels de generella processerna för att styra och leda informationssäkerhetsarbetet på strategisk och taktisk nivå, det vill säga ledningssystemet för informationssäkerhet (LIS). En generell process som går från strategisk till operativ nivå är tex. riskhantering och en operativ process kan vara ändringshantering.

De berörda operativa verksamhetsprocesserna kan vara:

- kontinuitetshantering
- informationsklassificering
- incidenthantering
- förändringshantering
- service och supporthantering
- behörighetshantering
- patch-hantering

Figur 1 visar interaktionen mellan ledningssystemet och de specifika säkerhetsprocesserna i informationssäkerhetsarbetet. De tomma pilarna visar de processer för informationssäkerhetsarbetet som finns på operativ nivå.

Figur 1. Informationssäkerhetsarbetet på strategisk, taktisk och operativ nivå



1.4 PDCA-modellen

En viktig utgångspunkt för processarbetet är att PDCA-modellen (”plan, do, check, act”) genomsyrar hela arbetet. Att planera, genomföra, följa upp och förbättra är grundstenarna för att ständigt förbättra processerna.

Genom att hela tiden arbeta med förbättringar och anpassningar kan verksamheten skapa ett system för informationssäkerhet som kan möta nya utmaningar och krav från omvärlden, exempelvis ny teknik, nya brottstrender och nya verksamhetsbehov. Ledningssystemet för informationssäkerhet bör innefatta PDCA-modellen enligt de övergripande stegen:

- Planering – Insamling av krav och målsättning samt framtagande av handlingsplan.
- Genomföra – Driva och genomföra det faktiska informationssäkerhetsarbetet.
- Följa upp- Mätning och uppföljning av krav och uppsatta mål för informationssäkerhetsarbetet.
- Förbättra – Resultat från uppföljningen ligger till underlag för kommande förbättringar och prioriteringar samt kompetensutveckling etc.

2. Vägledning för att utforma processer

2.1 Förberedelser

Innan man börjar arbetet med att utforma processer är det viktigt att tydliggöra de formella faktorerna och få klarhet i följande frågeställningar:

- Vem är beställare eller uppdragsgivare för arbetet?
- Vem är ansvarig för att det finns processer och för att informationssäkerhetsarbetet fungerar?
- Vem ska leda arbetet med att ta fram säkerhetsprocesserna?
- Vilka ska ingå i framtagandet av säkerhetsprocesserna, det vill säga processanalysgruppen? (En rekommendation är att ta med medarbetare från säkerhet, IT och verksamheten för att det ska fungera.)

2.2 Planering

Planeringen går främst ut på att sätta ihop de arbetsgrupper som ska identifiera och ta fram säkerhetsprocesserna. Det är viktigt att arbetsgruppen har en bred samlad kompetens och representerar hela organisationen. En viktig del i planeringen är att boka lämpliga lokaler för arbetet och att skaffa fram den utrustning och det arbetsmaterial som behövs under arbetsmötena.

Följande aktiviteter bör genomföras under planeringen:

- Se över analysgruppens sammansättning.
- Ta fram informationsunderlag inför analysen. Det är underlag från den grundläggande analysen och annat underlag som kan finnas om hur säkerhetsarbetet bedrivs i verksamheten.
- Boka lokaler och orda fram utrustning.
- Ta fram en tidsplanering för arbetet.

2.3 Genomförande

Arbetet med att utforma processerna består i huvudsak av att besvara frågorna vad, varför, vem, var, när och hur. Oftast gör deltagarna detta under gemensamma arbetsmöten. Framtagandet av processerna bygger på följande grundläggande aktiviteter:

Identifiera processerna och etablera en ansvarig person.

- Specificera de processer som är viktiga för verksamheten och som bör prioriteras.
- Specificera och fastställ en processansvarig person som har helhetsansvaret för processen samt befogenheter att utveckla den.
- Säkerställ en arbetsgrupp som också kan delta i arbetet med att utveckla och styra processen.

Kartlägg processen samt genomför omedelbara förbättringar om det behövs.

- Identifiera krav och mål för processen med respektive intressenter.
- Identifiera en ansvarig person för processen samt dess avgränsning, mottagare, indata och utdata.
- Identifiera och kartlägg viktiga aktiviteter och flöden.
- Identifiera eventuella brister som kan förbättras eller justeras omedelbart.
- Säkerställ ett tydligt processdokument med ett detaljerat flödesschema.

Värdera och förbättra processen (gäller processer som är i förvaltning).

- Säkerställ relevanta mätningar för att utvärdera processen gentemot de ställda kraven. Ni kan finna tips om mätning i standarden ISO 27004.
- Se om utvärderingen visar några förbättringar för processen.

3. Arbetsuppgifter

3.1 Identifiera vilka säkerhetsåtgärder som kräver processer

Det första momentet går ut på att identifiera vilka säkerhetsåtgärder som kräver processer inom informationssäkerhetsarbetet. Verksamheten måste då gå igenom listan för de fastställda säkerhetsåtgärderna och markera vilka som kan tänkas behöva förutbestämda, dokumenterade och länkade aktiviteter som ska upprätthållas. Man kan samtidigt notera om det redan finns en process som kan uppdateras för att tillgodose kraven på den nya säkerhetsåtgärden. Det är också en god idé att prioritera processerna enligt deras betydelse för verksamheten. (Bilaga C visar exempel på en övergripande processkarta för att identifiera säkerhetsprocesser.)

När det finns en förteckning över processerna som ska tas fram, eller uppdateras, bör arbetsgruppen även fastställa syftet samt indata och utdata för varje process. Detta är viktig information för nästa delmoment i utformandet av säkerhetsprocesserna. Dessutom måste verksamhetens chefer tidigt fastställa en ansvarig för varje process. Det är också bra att få ett formellt beslut från verksamhetsledningen om vilka processer som ska tillämpas.

Tillvägagångssätt:

- Identifiera processerna från säkerhetsåtgärderna.
- Prioritera säkerhetsprocesserna.
- Fastställ syfte, indata och utdata för varje process.
- Bestäm vilka säkerhetsprocesser som ska tillämpas.

Resultat av arbetsuppgiften:

Arbetsuppgiften är klar när det finns

- en förteckning som anger vilka processer som är viktiga i verksamheten (förslag på mall finns i bilaga A)
- syfte, indata och utdata för varje utvald process
- beslut om vilka processer som ska tillämpas.

3.2 Kartlägg varje befintlig process

Ofta finns redan någon form av process eller ett flöde för flera av säkerhetsåtgärderna man beslutade att införa i det förra delmomentet, men det är inte säkert att dessa processer är tydligt definierade och dokumenterade. I så fall är det dags att ta fram de fakta som finns och utgå från det vid processkartläggningen.

Arbetsgruppen ska använda den information som finns om varje process, det vill säga syftet med processen samt dess indata och utdata. Dessa parametrar anger omfattningen av processen och arbetsgruppen kan då börja kartlägga vilka aktiviteter som sker stegvis i nuläget, från indata till utdata. Denna övning kan göras genom att använda post-it-lappar för varje identifierad aktivitet och sätta dem i rätt ordningsföljd från indata till slutlig utdata. Dokumentationen kan bestå av flödesdiagram eller en lista över länkade aktiviteter.

När kartläggningen är klar kan arbetsgruppen även ta fram förslag till omedelbara förbättringar om man eventuellt har upptäckt svagheter eller brister på aktiviteterna i sig eller i deras ordningsföljd. Det är också bra att validera resultatet från arbetsgruppen mot verksamheten. Detta kan arbetsgruppen göra genom att ha avstämningar med de verksamhetsområden som påverkas av processen.

Tillvägagångssätt:

- Identifiera utdata, kravställare och kraven för processen.
- Definiera processens syfte och avgränsningar.
- Identifiera indata och intressenter.
- Identifiera processtegen (aktiviteter och flöden).
- Gör eventuellt omedelbara förbättringar och justeringar.
- Validera processkartläggningen.

Resultat av arbetsuppgiften

Arbetsuppgiften är klar när det finns

- en dokumenterad processkartläggning (förslag på mall finns i bilaga B)
- ett detaljerat flödesschema med aktiviteter.

3.3 Kartlägg varje ny process

I det här momentet ska arbetsgruppen kartlägga de ”nya” processerna – de processer som inte finns, men som man har beslutat att tillämpa. Det görs på liknande sätt som kartläggningen av de befintliga säkerhetsprocesserna, men utan steget ”omedelbara förbättringar”. Arbetsgruppen ”brainstormar” fram de aktiviteter som måste finnas för att gå från indata till utdata. Processerna bör dokumenteras så att det blir lätt att förklara dem för alla berörda parter innan de sätts i verket.

Tillvägagångssätt:

- Identifiera utdata, kravställare och kraven för processen.
- Definiera processens syfte och avgränsningar.
- Identifiera indata och intressenter.
- Identifiera processtegen (aktiviteter och flöden).
- Validera processkartläggningen.

Resultat av arbetsuppgiften

Arbetsuppgiften är klar när det finns

- en dokumenterad processkartläggning (förslag på mall finns i bilaga A).
- ett detaljerat flödesschema med aktiviteter.

4. Nästa steg

Detta delmoment är färdigt när säkerhetsprocesserna är dokumenterade och klara. Då blir nästa steg att utforma policy- och styrdokument.

Bilaga A: Mall för att identifiera säkerhetsprocesser

Denna mall kan användas för att dokumentera identifieringen av säkerhetsprocesserna.

Tabell A1. Identifiering och dokumentation av säkerhetsprocesserna

Prioritet	Säkerhetsprocess/ säkerhetsåtgärd	Syfte	Indata	Utdata	Anteckning

Bilaga B: Mall för processkartläggning

Denna mall kan användas för att kartlägga processen. Komplettera eventuellt med ett detaljerat flödesschema.

Tabell B1. Kartläggning av processer

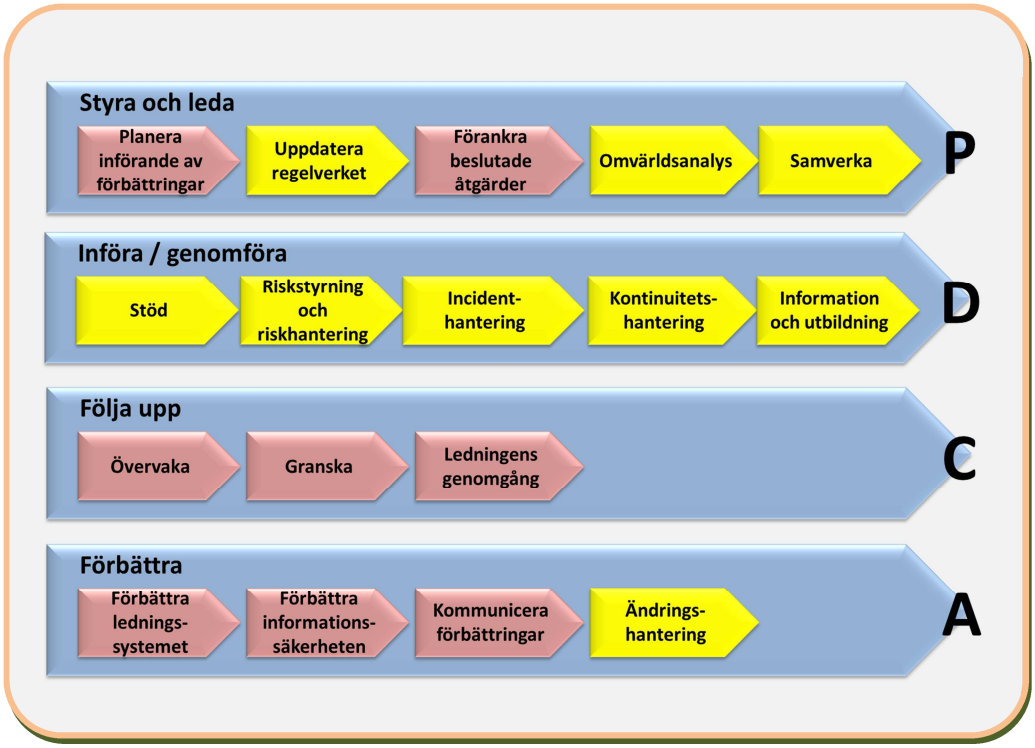
Processnamn:		[Processens benämning.]
Beskrivning:		[Beskriv kort processen samt dess omfattning och avgränsningar. Ge en definition av processen.]
Syfte:		[Beskriv kort processens syfte för verksamheten och informationssäkerhetsarbetet. Ange varför processen behövs.]
Mål:		[Beskriv kort processens mål för verksamheten och informationssäkerhetsarbetet. Ange effekten eller slutresultatet från processen.]
Krav:		[Beskriv kort vem som ställer krav och vilka kraven är för processen.]
Processägare/ Ansvarig:		[Ange vem som är ägare och ansvarig för processen.]
Mätning:		[Ange vad som ska mätas och vilka mätmål som finns för processen. Ange vilken prestanda processen ska ha.]
Indata:		[Ange vilken indata som initierar eller triggar denna process.]
Utdata:		[Ange utfallet, dvs. utdata. Ange med andra ord resultatet från denna process.]
Processteg		
1	**[Processteg 1]**	[Beskriv kort processteget med tillhörande aktiviteter.]
2	**[Processteg 2]**	[Beskriv kort processteget med tillhörande aktiviteter.]
3	**[Processteg 3]**	[Beskriv kort processteget med tillhörande aktiviteter.]
4	**[Processteg 4]**	[Beskriv kort processteget med tillhörande aktiviteter.]
5	**[Processteg 5]**	[Beskriv kort processteget med tillhörande aktiviteter.]
Intressenter:		[Ange processens främsta intressenter i verksamheten – roller, styrgrupper, avdelningar, andra processer etc.]
Information:		[Ange vilken information processen kräver och de styrdokument som finns.]
Stöd:		[Ange vilket stöd processen behöver för att fungera – utrustning, utrymme, system, metoder, resurser etc.]
Förbättringar:		[Beskriv kort omedelbara förslag på förbättringar.]
Övrigt:		[Ange kort annan information som är viktig för denna process.]

Bilaga C: Processkarta över LIS med delprocesser

För att identifiera och kartlägga processerna är det viktigt att ha en övergripande processkarta över LIS huvudprocesser med respektive delprocesser och specifika säkerhetsprocesser.

Nedanstående bild är ett exempel på en övergripande karta över de processer som kan behövas inom informationssäkerhetsarbetet. I denna karta framgår både processer som stöttar själva LIS-arbetet (de röda pilarna) och operativa säkerhetsprocesser för att införa och genomföra (de gula pilarna).

Figur C1: Bilden beskriver processer för informationssäkerhetsarbetet.



En förteckning över LIS kan t.ex. innehålla följande delprocesser och specifika säkerhetsprocesser:

1. **Styra och leda informationssäkerhetsarbetet**
    a. Planera införandet av förbättringar
    b. Uppdatera regelverk
    c. Göra omvärldsanalyser
    d. Förankra beslutade åtgärder
    e. Samverka externt och internt
2. **Införa eller genomföra informationssäkerhetsarbetet**
    a. Stödja verksamheten
    b. Riskstyr och riskhantera
    c. Incidenthantera
    d. Kontinuitetshantera
    e. Informera och utbilda
    f. Övervaka och loggningshantera
3. **Följa upp informationssäkerhetsarbetet**
    a. Mäta gentemot de framtagna indikatorerna för informationssäkerheten
    b. Granska och följa upp åtgärder
    c. Gå igenom informationssäkerheten (ledningen)
4. **Verksamhetsutveckla informationssäkerhetsarbetet**
    a. Förbättra ledningssystemet
    b. Förbättra säkerhetsprocesserna
    c. Kommunicera förbättringsåtgärder
    d. Hantera ändringar