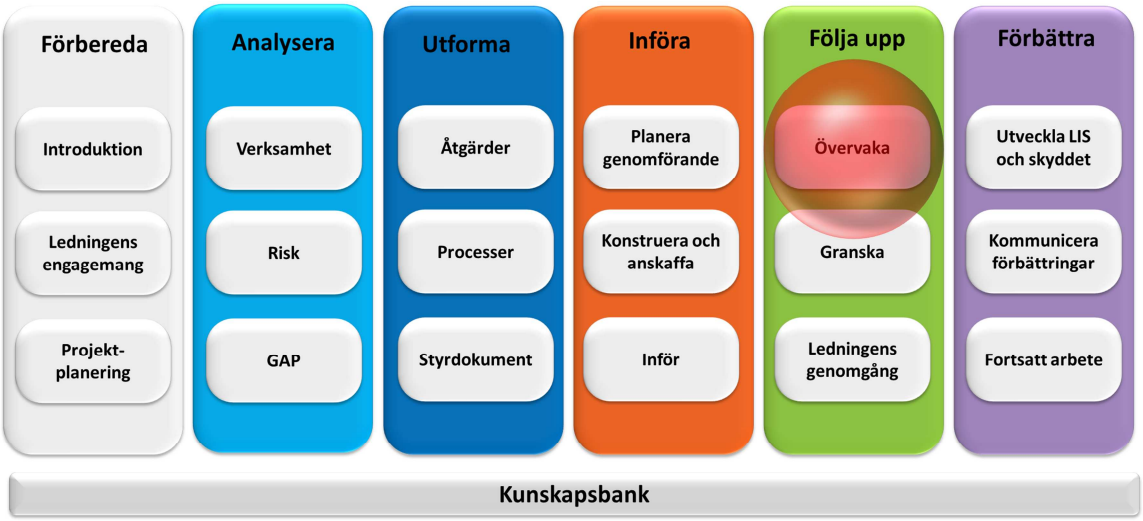
Myndigheten för samhällsskydd och beredskap

Övervaka



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

För att kunna veta om organisationens ledningssystem och dess informationssäkerhet är ändamålsenligt utformat och har avsedd verkan krävs övervakning och mätning.

Organisationen måste först avgöra *vad* som ska övervakas och mätas. Man måste också avgöra *hur* och *när* man ska övervaka, mäta, analysera och utvärdera för att få relevant och tillförlitlig information om informationssäkerheten.

Genom löpande övervakning och mätning kan organisationen få visshet om att informationssäkerheten är god eller upptäcka att något måste göras för att korrigera brister.

Den övervakning som diskuteras här handlar *inte* om övervakning av personal utan om övervakning av att ledningssystemet för informationssäkerhet och de säkerhetsåtgärder man beslutat om är ändamålsenligt och har avsedd verkan respektive existerar och fungerar tillfredsställande.

Det finns alltid någon form övervakning på plats i verksamheten innan detta steg tas. Ofta är situationen sådan att övervakningen har svagheter så som:

- Man har inte på ett strukturerat sätt beslutat vad man har *behov* av att övervaka.
- Man har inte beslutat på vilket sätt övervakning ska ske.
- Information från övervakningen analyseras inte i efterhand så att slutsatser kan dras.

Det är sådana svagheter som kan lösas genom tillämpning av detta steg.

2. Mål med mätning och övervakning

De övergripande målen med mätning och övervakning vad gäller ledningssystem för informationssäkerhet är:

1) **Ledningssystemet**: Att skapa förutsättningar för att utvärdera ledningssystemets ändamålsenlighet och verkan.

2) **Säkerhetsåtgärderna**: Att skapa förutsättningar för att utvärdera implementerade säkerhetsåtgärder och säkerhetsprocessers ändamålsenlighet och verkan.

3) **Informationstillgångarna**: Att skapa förutsättningar för att kunna upptäcka och utvärdera påverkan på informationstillgångarna i form av bristande sekretess, riktighet och tillgänglighet.

Information från mätning och övervakning kommer i senare skeden att ligga till grund för *granskning* och *ledningens genomgång*, vilka är de två kommande stegen efter detta.

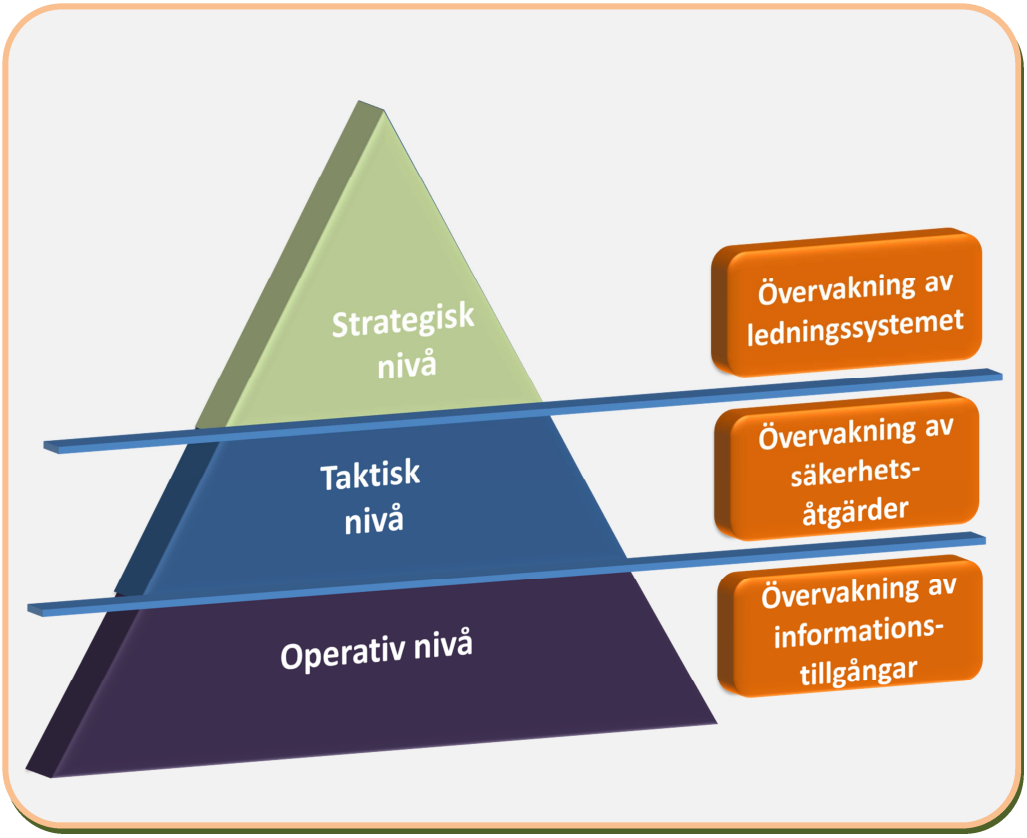
Mätning och övervakning på tre olika nivåer kan utskiljas, kopplat till de tre målen ovan, se nästa avsnitt.

3. Nivåer av övervakning

Övervakning av informationssäkerheten kan ske på flera olika nivåer och med olika tidsperspektiv:

- **Operativ** nivå: Löpande övervakning med fokus på informationens säkerhet.
- **Taktisk** nivå: Övervakning av att beslutade säkerhetsåtgärder existerar och fungerar tillfredsställande.
- **Strategisk** nivå: Övervakning av att ledningssystemet för informationssäkerhet är adekvat utformat och fungerar ändamålsenligt.

Figur 1. Övervakning kan ske på olika nivåer i verksamheten



3.1 Operativ övervakning - informationstillgångarnas säkerhet

På den operativa nivån övervakas säkerheten för de informationstillgångar som ska åtnjuta det skydd som beslutats. Denna typ av övervakning bygger i huvudsak på loggning av händelser i IT-system.

Exempel: I säkerhetsloggen, som utgör del av övervakningen, på server x har noterats att någon försökt logga in med fel lösenord på ett administrativt konto upprepade gånger mellan klockan 02:23 och 04:43 igår natt.

3.2 Taktisk övervakning - säkerhetsåtgärdernas effektivitet

Varje säkerhetsåtgärd innehåller inslag av sådant som kan övervakas, så att man genom manuell eller automatiserad övervakning kan tillse att en enskild beslutad säkerhetsåtgärd existerar och fungerar tillfredsställande i olika delar av verksamheten.

Exempel: I samband med en IT-revision upptäcks att loggning på en grupp servrar inte är påslagen trots att ledningssystemet föreskriver viss typ av loggning för de aktuella servrarna, det vill säga den beslutade säkerhetsåtgärden är inte i kraft.

3.3 Strategisk övervakning - ledningssystemets effektivitet

Utöver säkerhetsåtgärderna behöver själva ledningssystemets olika komponenter övervakas. Här handlar det om övervakning av de övergripande styrande mekanismerna. Fokus på den strategiska övervakningen är såväl internt som externt (Hur påverkar förändringar i omvärlden vårt behov av informationssäkerhet?)

Exempel: Hur påverkar förändringar i omvärlden vårt behov av informationssäkerhet? Identifieras nya risker så att skyddet kan kompletteras?

4. Faktorer som inverkar

Exakt hur verksamheten bör utforma sitt program för övervakning och mätning beror på följande faktorer:

1) verksamhetens behov
2) krav från avtal och författning
3) kostnader och nytta med övervakning och mätning
4) IT-tekniska och organisatoriska förutsättningar.

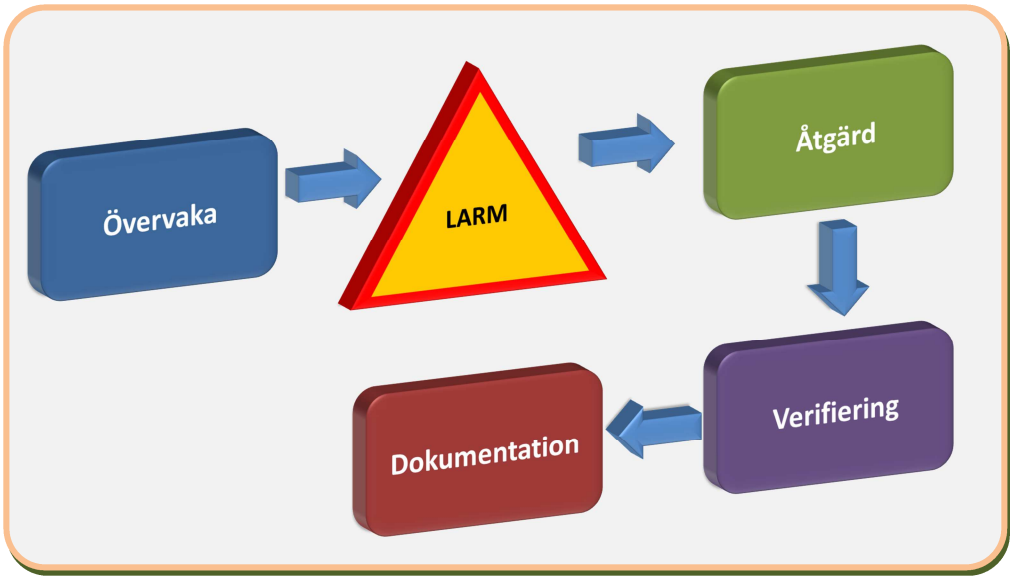
Att kontinuerligt mäta och övervaka olika objekt kostar resurser. Därför kan man inte mäta och övervaka allt. Istället måste man välja ut de viktigaste objekten och mätpunkterna.

Verksamhetens behov är den första utgångspunkten som ska avgöra vad som ska mätas, hur och när. För att komplettera detta måste krav från avtal och författning också beaktas – vissa händelser måste kanske övervakas och rapporteras till tillsynsmyndighet, eller av annat skäl. Sedan är det alltid en ekonomisk fråga där man måste ställa kostnaden för mätningen mot den nytta mätningen kan tänkas medföra. Därtill får man lägga de restriktioner som teknik och organisation ger – allt man skulle vilja övervaka kanske inte går att övervaka.

5. Övervakning som del av incidenthantering

När övervakningen visar en eventuell avvikelse måste den hanteras. Därför finns övervakningen i ett speciellt sammanhang i organisationen.

Figur 2. Övervakningen i sitt sammanhang



Som figuren visar är övervakningen en del av verksamhetens incidenthantering. Här beskrivs ett typiskt sådant flöde:

1. **Övervakning**: Övervakningen noterar en händelse i någon form av logg.
2. **Larm**: En automatisk eller manuell läsning av loggen identifierar händelsen som en avvikelse, och meddelar detta i form av ett "larm".
3. **Åtgärd**: Avvikelsen åtgärdas. Hur det går till beror på hur verksamhetens incidenthantering är organiserad (incidenthantering är en av de säkerhetsprocesser som tas upp i tidigare steg). Incidenthanteringen bör innefatta principer för hur avvikelser ska larmas och hanteras i verksamheten.
4. **Verifiering**: När en åtgärd är införd måste man se till att åtgärden har rätt effekt, det vill säga att den verkligen åtgärdar avvikelsen.
5. **Dokumentation**: Det hela dokumenteras så att man kan lära sig av det inträffade, och i efterhand kan granska avvikelserna och hur de hanterades. Detta dokumenteras ofta i datoriserade eller manuella incidenthanteringssystem, och de är en viktig datakälla för efterföljande analyser och granskning (vilket behandlas i nästa aktivitet i metoden – *granska*).

6. Teknisk övervakning

Teknisk övervakning är alla automatiserade sätt att övervaka säkerheten för verksamhetens informationstillgångar. Oftast har man teknisk övervakning på den operativa nivån (figur 2). Det finns olika typer av teknisk övervakning och nedan nämns några exempel.

6.1 Driftövervakning

Driftövervakningen används för att övervaka verksamhetens IT-system, främst när det gäller tillgängligheten. Övervakningen kan visa att hårdvaran är fullt fungerande och har nog med kapacitet (till exempel hårddiskar, processorer, internminne och kommunikationslänkar). Driftövervakningen gäller också annat än hårdvara, som databashanterare, webbservrar och tillämpnings-program. Denna övervakning indikerar kontinuerligt ifall de övervakade komponenterna är tillgängliga, har den kapacitet som behövs och fungerar som förväntat.

Driftövervakningen ska till exempel larma om

- en hårddisk går sönder
- temperaturen i en server stiger onormalt
- en webbserver slutar att servera hemsidan till besökare.

6.2 Loggning

En annan typ av övervakning är loggning, vilket innebär att en fil (oftast en vanlig textfil) lagrar uppgifter om en händelse med tidpunkt och vilka resurser som var inblandade. Information loggas hela tiden på olika sätt, oavsett om det är genomtänkt eller inte. Loggning kan dock nästan alltid skräddarsys för att passa verksamhetens behov. Det är viktigt att loggarna skyddas på ett lämpligt sätt och att de inte kan ändras av någon som vill dölja en händelse. Vissa verksamheter väljer därför att samla in alla loggar centralt till en plats.

Ett loggningssystem kan till exempel övervaka

- operativsystem
- databashanterare och applikationsservrar
- applikationer.

Loggarna kan bland annat innehålla information om tid och plats för en inloggning, problem och fel som har identifierats samt vem som har tagit del av vilken information.

7. Manuell övervakning

Med manuell övervakning menas här all övervakning som sker manuellt med hjälp av personalinsatser.

Den här övervakningsformen gäller oftast de taktiska och strategiska nivåerna i figur 2. Övervakningen ska alltså se till att säkerhetsåtgärderna finns på plats och att ledningssystemet är effektivt.

Med manuell övervakning kan man till exempel kontrollera att

- blanketter för behörighetsutdelning är korrekt ifyllda
- nya risker mot en specifik verksamhet eller informationstillgång är hanterade (genom att göra en riskanalys).

8. Ytterligare stöd

Ledningssystemstandarden ISO/IEC 27001 ger viss information om krav på mätning och övervakning i avsnittet 4.2.

Det finns också en separat standard gällande hur man utformar ett program för den mätning och övervakning som avses här. Den heter ISO/IEC 27004, och är till stor hjälp i det här steget.

9. Nästa steg

Nu har verksamheten ett väl fungerande sätt att övervaka säkerhetsåtgärder och säkerhetsprocesser. Då gäller det att mer långsiktigt analysera och dra slutsatser av de loggar och larm som skapas i aktiviteten *övervaka*. Bland annat detta görs i nästa aktivitet – *granska*.