Myndigheten för samhällsskydd och beredskap

Innehållsförteckning

1 Utforma

1.1 [Utforma] Organisationens säkerhetsåtgärder

Målet med det systematiska informationssäkerhetsarbetet är att införa och förbättra de säkerhetsåtgärder som organisationen behöver. Förutsättningarna för säker hantering av information förändras ständigt och säkerhetsåtgärderna behöver återkommande anpassas till nya krav, hot och behov. Därför behöver man arbeta systematiskt och utifrån bedömda risker med att förstå vilka säkerhetsåtgärder som behövs, införa dem, och följa upp att de fungerar som det var tänkt.

Den här vägledningen beskriver hur du kan utforma ert arbete med säkerhetsåtgärder.

- Du hittar stöd för hur du analyserar vilka säkerhetsåtgärder ni behöver i **Identifiera och analysera Organisationens säkerhetsåtgärder.**
- I **Utforma Gruppera säkerhetsåtgärder i skyddsnivåer** beskrivs hur du kan gruppera säkerhetsåtgärder i skyddsnivåer och koppla dem mot konsekvensnivåerna i organisationens klassningsmodell.
- I **Använda Organisationens säkerhetsåtgärder** beskrivs hur säkerhetsåtgärder anpassas för att ge tillräckligt skydd för informationen och informationsbehandlande resurser.

1.1.1 Vad är en säkerhetsåtgärd?

En säkerhetsåtgärd är en åtgärd som syftar till att säkerställa att något värdefullt i organisationen har tillräckligt skydd. Arbete med att förstå vilka säkerhetsåtgärder som en organisation behöver görs inte bara inom informationssäkerhetsarbetet utan också för att skydda värden inom andra områden till exempel skyddsutrustning för en säker arbetsmiljö, lås och larm för fysiska tillgångar, brandskydd för lokaler.

En säkerhetsåtgärd som skyddar inom ett område kan också ge skydd inom ett annat. Till exempel skyddar fysiska säkerhetsåtgärder såsom dörrar, lås och larm som införts för att skydda organisationens lokaler och personal också information som behandlas i lokalerna. Säkerhetsåtgärder kan införas på olika sätt, i olika grad och ofta behövs en kombination av flera säkerhetsåtgärder för att ge det skydd som behövs.

1.1.1.1 Säkerhetsåtgärder och risk

Säkerhetsåtgärder införs för att minska (reducera) eller helt ta bort (eliminera) risker (se **Utforma Riskhantering**). Det innebär att den som äger en risk blir beroende av att den som ges ansvar för en säkerhetsåtgärd faktiskt också inför säkerhetsåtgärden så att den fungerar väl.

Ansvaret för säkerhetsåtgärder behöver beskrivas tydligt i förhållande till ansvar för risker inom organisationen:

- En riskägare som inte kan påverka hur väl säkerhetsåtgärder blir införda blir bakbunden i sitt ansvar.
- En ansvarig för säkerhetsåtgärder som inte kan påverka vilka eller hur mycket resurser som tilldelas kan sannolikt inte införa de säkerhetsåtgärder som riskägaren kravställt på det sätt som de behöver införas.

Därför är det extra viktigt att styrande dokument och arbetssätt skapar förutsättningar för de personer som innehar dessa roller att, utifrån sitt ansvar, hantera behovet av säkerhetsåtgärder på ett effektivt sätt och att frågor som inte kan lösas inom eller mellan rollerna enkelt kan eskaleras (se **Utforma Riskhantering** och **Utforma Organisation**).

Exempel: Samverkan mellan riskägare och åtgärdsansvarig

En avdelningschef är ägare till risken att känslig information läcker till obehöriga därför att det saknas lås till arkivrummet. Fastighetsägaren har fått ansvar för säkerhetsåtgärden ”lås på dörrar”. Resurser som kan installera lås på dörrar finns hos chefen för kontorsservice.

Risken kommer inte att minska så fort avdelningschefen beslutar att risken ska åtgärdas genom att lås ska installeras på dörren. Fastighetsägaren behöver utifrån beslutet prioritera att köpa in rätt lås, skapa nödvändiga instruktioner för utlämning av nycklar med mera och begära resurser för att installera låsen.

Därefter behöver chefen för kontorsservice prioritera att tilldela de begärda resurserna för att genomföra installationen. Först när alla led har gjort det som behövs har risken minskats. Riskägaren behöver bevaka att risken åtgärdas och ha möjlighet att eskalera om säkerhetsåtgärden inte införs inom den tid som riskägaren kan acceptera. Eventuellt behöver information om att riskägaren har en risk eskaleras om risken bedöms vara tillräckligt allvarlig.

1.1.1.2 Vad är en informationssäkerhetsåtgärd?

Informationssäkerhetsåtgärder syftar till att skydda information så att konfidentialitet, riktighet och tillgänglighet upprätthålls. De syftar också till att skydda de resurser som behandlar informationen, såsom it-system, nätverk och personal, genom till exempel säkerhetsåtgärderna brandvägg, nätverkssegmentering och utbildning. I den här vägledningen kallas informationssäkerhetsåtgärder för säkerhetsåtgärder.

1.1.1.3 Två huvudtyper av säkerhetsåtgärder inom informationssäkerhet

Begreppet säkerhetsåtgärd används för en stor mängd åtgärder av olika slag som leder till ökad säkerhet för information och de resurser som hanterar information. Säkerhetsåtgärderna kan sägas vara av olika karaktär, användas på många olika sätt och att kategorisera dem kan av olika skäl vara till hjälp (se nedan Kategorisering av säkerhetsåtgärder). Det finns skäl att redan här skilja mellan två huvudtyper av säkerhetsåtgärder, därför att arbetet med dem skiljer sig åt på några avgörande sätt.

1.1.1.3.1 Säkerhetsåtgärder för informationsbehandling

Den ena typen, som i den här vägledningen kallas ”säkerhetsåtgärder för informationsbehandling”, leder direkt till ökad säkerhet för information och de informationsbehandlande resurserna när de är införda och fungerar väl. Exempel på sådana säkerhetsåtgärder är

- instruktioner för behörighetshantering
- införda brandväggskonfigurationer
- utbildning i hur organisationens datorer får användas
- lås och larm.

Införda säkerhetsåtgärder för informationsbehandling utgör skydd för er information och de resurser som behandlar den. Varje säkerhetsåtgärd anpassas av den som får ansvar för säkerhetsåtgärden baserat på underlag och beslut från organisationens arbete med klassning, risk och säkerhetsåtgärder. Detta är resultatet av informationssäkerhetsarbetet. Du hittar stöd för hur ni arbetar med att anpassa säkerhetsåtgärderna så ger tillräckligt skydd utifrån organisationens behov i metodsteget **Använda Organisationens säkerhetsåtgärder**.

1.1.1.3.2 Säkerhetsåtgärder för styrning

Den andra typen, som i denna vägledning kallas för ”säkerhetsåtgärder för styrning”, innebär en indirekt säkerhet när de är införda och fungerar väl. De handlar om att leda och samordna informationssäkerhetsarbetet och skapar förutsättningar som gör det möjligt för din organisation att välja rätt säkerhetsåtgärder för informationsbehandling. Säkerhetsåtgärder för styrning syftar alltså till att göra säkerhetsåtgärderna för informationsbehandling kostnadseffektiva, det vill säga att skyddet är tillräckligt utifrån era behov, men inte kostar mer än nödvändigt. Exempel på säkerhetsåtgärder för styrning är

- att ansvar och roller är specificerade
- att det finns en informationssäkerhetspolicy som ger ledningens inriktning för arbetet
- att organisationen genomför informationsklassningar och riskbedömningar.

Till säkerhetsåtgärder för styrning räknas i denna vägledning även risk-, incident- och kontinuitetshantering. Dessa säkerhetsåtgärder relaterar till ledningssystem på andra områden och behöver integreras med dessa så långt det är möjligt.

De säkerhetsåtgärder för styrning som organisationen har infört är grunden för ert systematiska informationssäkerhetsarbete. Dessa utformas till största del av dig som CISO och beslutas i många fall av organisationens ledning eftersom de påverkar hela organisationen på ett eller annat sätt.

1.1.1.4 Vad är tillräckligt skydd?

Skydd för information handlar som tidigare nämnts om att säkerställa att informationens konfidentialitet, riktighet och tillgänglighet upprätthålls så att

- endast behöriga har åtkomst till informationen
- det går att lita på att informationen inte är obehörigt ändrad
- den är tillgänglig när behöriga användare behöver den.

Vad som är tillräckligt skydd beror bland annat på

- organisationens mål
- krav på organisationen
- vilka verksamheter som bedrivs
- hur villig ledningen är att ta risker med att informationen blir åtkomlig för obehöriga, att den blivit inkorrekt eller inte går att komma åt när den behövs.

1.1.1.5 Vad innebär införd och fungerar väl?

I gapanalysen kontrollerar du om en säkerhetsåtgärd är införd och fungerar väl (**Identifiera och analysera Organisationens säkerhetsåtgärder**). En säkerhetsåtgärd kan sägas vara införd när den har dokumenterats i ett beslutat styrdokument. Då ”finns” säkerhetsåtgärden i organisationen. Men det innebär inte att någon ytterligare säkerhet har uppnåtts. För att säkerheten ska uppnås krävs att säkerhetsåtgärden också fungerar väl.

För att säkerhetsåtgärder ska fungera väl krävs att säkerhetsåtgärden:

1. **har anpassats** till organisationen genom att detaljeras utifrån era behov så att det blir möjligt för de det gäller att *tillämpa* säkerhetsåtgärden.
2. **faktiskt tillämpas** i organisationen
3. **följs upp och utvärderas**
4. **faktiskt motverkar risken** och fortfarande är tillräcklig

Först när alla dessa mål har uppnåtts kan säkerhetsåtgärden sägas fungera väl.

1.1.1.6 Begreppsförklaringar

Nedan följer en lista på begrepp som används i metodstödets vägledningar om säkerhetsåtgärder (se också **Identifiera och analysera Organisationens säkerhetsåtgärder**, **Använda Organisationens säkerhetsåtgärder**) och hur vi har valt att använda begreppen. Observera att det inte är några definitioner, utan begreppsförklaringar.

- Gapanalys – metod för att undersöka skillnaden, gapet, mellan hur något är och hur det borde vara.
- Säkerhetsåtgärder – åtgärder för att minska risker och skydda värden (andra begrepp för säkerhetsåtgärder kan till exempel vara skyddsåtgärder, eller bara åtgärder).
- Lämpliga säkerhetsåtgärder – säkerhetsåtgärder som minskar risken så att skyddet blir tillräckligt
- Tillämpliga säkerhetsåtgärder (UoT/SoA) – de säkerhetsåtgärder som analyser visat att organisationen behöver (se **Identifiera och analysera Organisationens säkerhetsåtgärder**).
- Säkerhetsåtgärder för styrning – säkerhetsåtgärder som innehåller organisationens styrning av informationssäkerhet och är beståndsdelar ett systematiskt informationssäkerhetsarbete
- Säkerhetsåtgärder för informationsbehandling – säkerhetsåtgärder som direkt skydda information och system för informationsbehandling.

1.1.1.7 Kategorisering av säkerhetsåtgärder – för att lättare förstå dem

Att kategorisera säkerhetsåtgärder kan hjälpa en organisation att förstå vad en viss säkerhetsåtgärd bidrar med till organisationen. Vilka kategorier som fungerar skiljer sig mellan organisationer, och kan även förändras över tid.

Olika sätt att kategorisera säkerhetsåtgärder:

1. **Efter åtgärdens syfte:** Åtgärder kan kategoriseras utifrån om de främst syftar till att minska sannolikheten för att en risk inträffar eller om de är inriktade på att minska konsekvenserna av en inträffad risk.
2. **Utifrån skyddsfokus:**
   - **Konfidentialitet:** Skydda känslig information från obehörig åtkomst.
   - **Riktighet:** Säkerställa att informationen är korrekt och tillförlitlig.
   - **Tillgänglighet:** Säkerställa att information och system är tillgängliga vid behov.
3. **Baserat på ansvar och insikt:**
   - Roll som kommer att vara ansvarig för en säkerhetsåtgärd.
   - Roll som kan veta mer om hur säkerhetsåtgärden fungerar.
4. **Efter typ av åtgärd:**
   - Organisatoriska åtgärder.
   - Administrativa åtgärder.
   - Personalrelaterade åtgärder.
   - Fysiska åtgärder.
   - Tekniska åtgärder.
5. **Efter åtgärdens funktion:**
   - Förebyggande åtgärder: Identifiera behov och skydda information innan en risk inträffar.
   - Hanterande åtgärder: Upptäcka, agera och återställa vid incidenter.

1.1.1.7.1 Praktiska överväganden vid kategorisering

Oavsett om ni väljer att använda färdiga kategorier eller skapar egna, är det viktigt att reflektera över vad varje åtgärd bidrar med till organisationens skydd. Om ni väljer att kategorisera åtgärder är det bra att vara flexibel, eftersom vissa säkerhetsåtgärder kan passa in i flera kategorier eller inte helt passa in i någon. Det är helt okej – kategorisering ska underlätta, inte försvåra.

Lägg inte för mycket tid på att hitta rätt kategori. Börja med en övergripande struktur och justera efter behov under arbetets gång. Målet är att skapa en användbar överblick över organisationens säkerhetsåtgärder och deras bidrag till helheten.

1.1.2 Varför arbeta med säkerhetsåtgärder för informationssäkerhet?

Vi arbetar med säkerhetsåtgärder för att få en effektiv och korrekt informationshantering. Säkerhetsåtgärderna införs för att hantera de risker som uppkommer om informationssäkerhetsarbetet inte fungerar tillräckligt väl eller om en viss informationsbehandling inte skyddas tillräckligt.

Allt vi gör inom informationssäkerhet, och som beskrivs i metodstödet, syftar till att *välja* rätt säkerhetsåtgärder, det vill säga de som ger tillräckligt skydd för informationen. Vad som

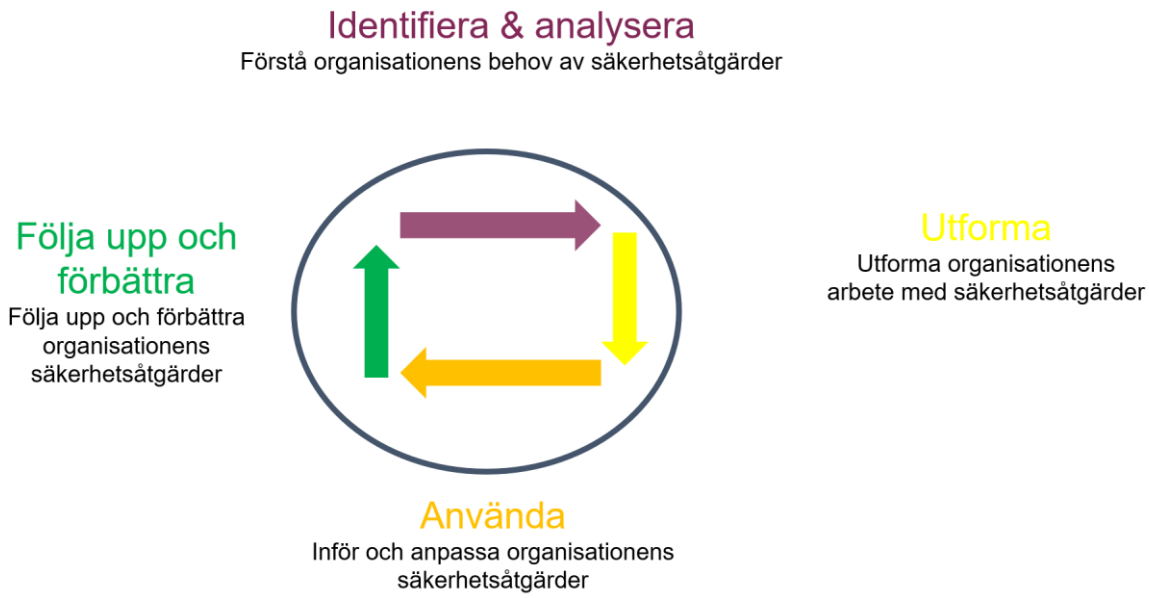
är en tillräcklig säkerhetsåtgärd beror på vilka mål som organisationen har, vilka risker som kan hindra måluppfyllnad och vilka interna och externa förutsättningar som finns.

Det är genom analyserna vi skapar underlag för att förstå de interna och externa förutsättningarna (**Identifiera och analysera Verksamhetsanalys och Omvärldsanalys**), värderar informationen (**Använda Klassa information**) och bedömer riskerna (**Använda Riskanalys)** för att förstå vilka säkerhetsåtgärder som behövs och hur de behöver anpassas. Skyddet uppstår först när säkerhetsåtgärderna är på plats och ger det avsedda skyddet. Därför måste vi utforma och införa de säkerhetsåtgärder som vi med hjälp av underlagen identifierat att vi behöver.

1.1.3 Arbeta med säkerhetsåtgärder

Vägledningen är utformad för att stödja det systematiska informationssäkerhetsarbetet med säkerhetsåtgärder. (se figur 1).

Figur 1: Arbetet med säkerhetsåtgärder relaterat till metodstödets steg



Den här vägledningen ger stöd i att utforma och etablera organisationens arbete med säkerhetsåtgärder.

Vägledningen kommer vid behov att anpassas för att utgöra ett stöd för att uppfylla kraven på systematiskt informations- och cybersäkerhetsarbete i cybersäkerhetslagen så att rätt säkerhetsåtgärder införs. Ytterligare stöd finns i standarder exempelvis:

- SS-EN ISO/IEC 27001 (krav) och SS-EN ISO/IEC 27002 Informationssäkerhet – cybersäkerhet och integritetsskydd - Informationssäkerhetsåtgärder)
- NIST Cybersecurity Framework
- IEC 62443 cybersecurity and control systems.

1.1.4 Utforma och etablera organisationens arbete med säkerhetsåtgärder

Börja med att identifiera om organisationen har etablerade arbetssätt för hur behov av säkerhetsåtgärder identifieras, prioriteras, införs och följs upp. Sök i styrdokument och fråga kollegor som arbetar med annan säkerhet för att hitta det som finns.

Bedöm om du kan använda befintliga arbetssätt som de är, om de kan justeras eller om du behöver ta fram helt nya arbetssätt för att ni ska ge tillräckligt skydd åt er information och de resurser som behandlar den.

Att utforma organisationens arbete med säkerhetsåtgärder innebär att skapa förutsättningar för att ni ska kunna anpassa och införa säkerhetsåtgärderna så att de fungerar väl. I vilken ordning du lämpligen utformar dina säkerhetsåtgärder beror på hur långt din organisation

har kommit i informationssäkerhetsarbetet och vilken väg som är möjlig att ta för er (se **Identifiera och analysera Organisationens säkerhetsåtgärder**).

En bra startpunkt, oavsett om du är organisationens första CISO eller om du tar över ett fungerande arbetssätt, är att arbeta för att säkerhetsåtgärderna Ledningens ansvar (se **Utforma Ledning och styrning**) och Informationssäkerhetspolicy (se **Utforma Styrdokument**) är införda och fungerar väl.

Att ha ett etablerat arbetssätt tillsammans med ledningen där de förstår både sin egen roll och ditt uppdrag underlättar din arbetssituation och skapar förutsättningar för god riskhantering i hela organisationen. Att ledningen beslutar om en informationssäkerhetspolicy ger ditt uppdrag validitet och en tydlighet när du möter den övriga organisationen.

Utgångspunkten för arbetet med att utforma organisationens säkerhetsåtgärder är genomförda analyser (**Identifiera och analysera Verksamhetsanalys, Omvärldsanalys och Organisationens säkerhetsåtgärder**) och huvudregeln är att så snart som möjligt börja med de säkerhetsåtgärder som motverkar de högsta riskerna. Det går dock inte alltid. Ibland behövs längre tid för att frigöra personal med rätt kompetens för arbetet.

Då kan det vara enklare att påbörja arbetet där det redan pågår aktiviteter inom organisationen och där det finns utrymme för att också ta hand om anpassningen av vissa säkerhetsåtgärder. Exempel på sådan aktivitet kan vara att HR-enheten ser över sitt introduktionsprogram för nyanställda och att du kan få med en grundläggande informationssäkerhetsutbildning i den, eller att it-enheten har påbörjat ett projekt för att förbättra övervakningen av it-miljön och att du kan få med krav på funktioner för säkerhetsövervakning.

När organisationen känner till att du finns och vad du kan hjälpa till med, ta väl vara på om någon del av organisationen visar engagemang för informationssäkerhet så kommer fler möjligheter öppna sig. Att stödja organisationen samtidigt som du skaffar kunskap om hur du bäst utformar olika säkerhetsåtgärder för styrning underlättar ditt arbete.

1.1.4.1 Exempel på sådana situation är att någon behöver hjälp med att värdera sin information – passa då på att testa ditt utkast till klassningsmodell. HR och organisationens jurist ser över arbets- och delegationsordningen, it enheten ska göra översyn av sitt arbetssätt för tilldelningen av behörigheter. Be att få delta och ta med dig de krav på säkerhetsåtgärder som har identifierats, och hjälp dina kollegor att också få med de anpassningar som behövs för att säkerhetsåtgärden ska fungera väl. Var dock noga med att det alltid är de som fått ansvar för en säkerhetsåtgärd som ska sköta arbetet med sina säkerhetsåtgärder. Ge det stöd som de behöver men ta inte över deras ansvar. Relationen till organisationens övriga arbete med säkerhetsåtgärder

I organisationer finns det medarbetare med andra roller som arbetar med att införa säkerhetsåtgärder. Du kan därför utgå ifrån att det finns en uppsättning säkerhetsåtgärder införda i din organisation för att skydda andra värden än information.

Där finns säkerhetsåtgärder som handlar om personalens arbetsmiljö, säker hantering av utrustning, skydd mot skadegörelse och mycket mer. I många fall kan en och samma

säkerhetsåtgärd skydda flera olika sorters tillgångar i organisationen. Exempel på sådana säkerhetsåtgärder är lås och larm, säkerhetsutbildningar och begränsning av åtkomst inom era lokaler.

Ibland kan en säkerhetsåtgärd skydda mot en sak och samtidigt riskera att orsaka skada på något annat. Exempelvis kan automatiska släckningssystem som använder vatten vara en utmärkt åtgärd för att släcka en brand, men om där finns it-utrustning kommer den att förstöras av vattnet. Då behöver ni välja något annat släckningsmaterial.

Det är viktigt att arbetet med säkerhetsåtgärder för information integreras med det befintliga säkerhetsarbetet. Det ökar effektiviteten både inom informationssäkerhetsarbetet och för resten av organisationen, främst genom att skapa en hållbar situation för de som ansvarar för att införa och förvalta säkerhetsåtgärder i organisationen.

1.1.4.2 Ansvar och roller

Runt arbetet med säkerhetsåtgärder är det särskilt tre roller som behöver ta ansvar för att säkerställa att arbetet är ändamålsenligt och att säkerhetsåtgärden i slutänden faktiskt tillämpas i organisationen.

- **Ansvarig för säkerhetsåtgärd** kallas den som får ansvar för att en säkerhetsåtgärd införs och fungerar väl. Den rollen ansvarar också för att följa upp och förbättra säkerhetsåtgärden så att den fungerar väl över tid. Det här ansvaret följer oftast med ansvaret för den verksamhet där säkerhetsåtgärden ska införas, följas upp och förbättras.
- **Den som ansvarar för att samordna organisationens arbete** med säkerhetsåtgärder kan vara en CISO, säkerhetschef eller motsvarande.
- **Riskägare** i form av informations- eller systemägare har ansvar för att identifiera vilket skydd som behövs för den information, och de resurser som hanterar information, som de ansvarar för (se **Utforma Organisation** respektive **Utforma Riskhantering**).

1.1.4.2.1 Ansvarig för en säkerhetsåtgärd

Ansvar för en säkerhetsåtgärd är ofta kopplat till ett befintligt ansvar i organisationen. Den som har ansvar för en säkerhetsåtgärd ansvarar för att den uppfyller organisationens behov utifrån de krav som externa och interna intressenter ställer. Samma roll har också ansvar för att åtgärden införs och följs upp samt förbättras så att den fungerar väl även över tid.

Den som är ansvarig för en säkerhetsåtgärd bidrar med kompetens och kunskap kring hur säkerhetsåtgärden kan anpassas, samt säkerställer resurser för att säkerhetsåtgärden förvaltas över tid.

Även om verksamhet utkontrakteras behöver det ändå finnas någon i organisationen som ansvarar för säkerhetsåtgärden. Ett skäl till detta är att organisationen måste veta vilka krav på säkerhetsåtgärder som ska ställas på leverantören och hur de ska följas upp av leverantören. I det här fallet är det leverantören som anpassar, följer upp och förbättrar säkerhetsåtgärden (se **Använda Organisationens säkerhetsåtgärder**). Ansvarig för säkerhetsåtgärden är då den inom organisationen som ställer krav på att det görs och att

information om hur väl säkerhetsåtgärden fungerar återkopplas från leverantören till organisationen.

Den i organisationen som är ansvarig för säkerhetsåtgärden ska också ha befogenhet och möjlighet att själv säkerställa att leverantören uppfyller de krav som har ställts. En oberoende granskning kan också säkerställa att leverantören uppfyller kraven.

1.1.4.2.1.1 Hur förstår du vem som är ansvarig för en säkerhetsåtgärd?

Det är inte alltid helt självklart vilken roll som bör ansvara för en viss säkerhetsåtgärd. Har du genomfört **Identifiera och analysera Verksamhetsanalys respektive Gapanalys** kan du hitta en del av svaren där. Börja med att identifiera den roll som nu har ansvaret för den verksamhet där en säkerhetsåtgärd ska införas. Den rollen kan vara den som bör ansvara för säkerhetsåtgärden. Ansvaret kan också läggs på den roll som har bäst förståelse för säkerhetsåtgärden.

Exempel på roller som kan ha ansvar för någon säkerhetsåtgärd är: it-chefen, HR-chefen och fastighetschefen men ansvaret kan också läggas på till exempel den it-säkerhetsansvariga, dataskyddsombudet, säkerskyddschefen, chefsjuristen eller arkivchefen.

Vissa säkerhetsåtgärder berör flera roller. Ibland passar ansvaret för en säkerhetsåtgärd in lika bra hos flera olika roller. Då är det bara att bestämma en roll och om det senare visar sig att ansvaret för säkerhetsåtgärden passar bättre någon annanstans, byta ansvarig.

Två exempel på ansvarsfördelning:

1. Ansvaret för säkerhetsåtgärden ”bakgrundskontroll” kan ligga antingen på HR-avdelningen eller på säkerhetsavdelningen. I det här fallet kan man tänka att HR ansvarar för allt som har med anställningar att göra och ansvaret ska ligga där eller att säkerhetsavdelningens kompetens gör att de bäst kan anpassa, genomföra och följa upp säkerhetsåtgärden.

   En enkel tumregel kan i dessa fall vara att ansvaret för säkerhetsåtgärden bör ligga så nära verksamheten som möjligt, men att de inblandade måste förstå beroendet till varandras ansvar och utforma tydliga överlämningspunkter. I exemplet är en sådan punkt där HR lämnar över att genomföra bakgrundskontroll till säkerhetsavdelningen som sedan återkopplar till HR när de är klara och kan redovisa ett resultat.

2. Ett annat exempel är de säkerhetsåtgärder som behöver införas och förvaltas i it-miljön. Där kan ansvaret ofta läggas på it-chefen, den it-säkerhetsansvariga eller motsvarande.

   Bestäm i dialog med de inblandade var det är bäst att ansvaret ligger. I ansvaret ingår att säkerställa att rätt resurser bidrar i arbetet, och att eskalera frågan om det finns risk att säkerhetsåtgärden inte kan införas enligt plan.

1.1.4.2.2 Rollen säkerhetschef eller motsvarande

I en del organisationer finns någon som har det övergripande ansvaret för organisationens säkerhet på alla områden. Denna roll ska också stötta de som är ansvariga för olika säkerhetsåtgärder och de som använder säkerhetsåtgärderna i sitt arbete med att nyttja säkerhetsåtgärderna på bästa sätt. Om det saknas en säkerhetschef eller motsvarande behöver du som CISO samordna säkerhetsåtgärder som syftar till att skydda information och resurser som behandlar information med säkerhetsåtgärder på andra områden.

Ansvarsförhållandena mellan de roller som ansvarar för olika delar av säkerheten i organisationen behöver tydliggöras i styrdokument, exempelvis ansvars- och delegationsordning, ansvarsprofil eller motsvarande.

1.1.4.2.3 Riskägarens roll

Riskägare i form av informationsägare bidrar främst till arbetet med säkerhetsåtgärder genom arbetet med klassning av information och riskanalys (se **Använda Klassning av information** respektive **Använda Riskanalys**). Det finns också ett ansvar för att följa upp att beslutade säkerhetsåtgärder införs enligt plan. I bästa fall har ni så bra stöd i till exempel användarhandböcker, modeller och etablerade arbetssätt att riskägaren teoretiskt sett inte behöver bidra med att förtydliga kraven på säkerhetsåtgärden ytterligare. Om säkerhetsåtgärder behöver förändras på något sätt för att fungera väl behöver informationsägaren och den som är ansvarig för säkerhetsåtgärden prata med varandra (undantagshantering).

Riskägare i form av systemägare ansvarar för skydda informationen såsom informationsägaren kravställt. Det gör systemägaren genom att själv bedöma risker med de säkerhetsåtgärder som denne infört för att skydda informationen och de informationsbehandlande resurserna som ingår i systemägarens ansvar. Systemägaren ställer samtidigt krav på att informationsägaren att ha tillräcklig kunskap om den information som ska behandlas i informationssystemen så att systemägaren kan ge det skydd som behövs. Ofta är det ändå så att det uppstår frågor om ifall säkerhetsåtgärderna som erbjuds är tillräckliga, hur säkerhetsåtgärderna bör anpassas eller hur kostnader för en säkerhetsåtgärd ska fördelas mellan den som ansvarar för den och den som använder den. I dessa lägen är det viktigt att samarbeta för att kunna införa ett tillräckligt bra skydd. Samarbete behövs också när en fråga behöver eskaleras så att det fattas medvetna beslut, ytterst i högsta ledningen, i frågor där den som har krav på skydd och den som ska erbjuda en säkerhetsåtgärd inte kommer överens om dess utformning. Läs mer om riskägarrollen i **Utforma Riskhantering**.

1.1.4.3 Att införa säkerhetsåtgärder genom styrdokument

Arbetet med att införa en säkerhetsåtgärd börjar i organisationens styrdokument. Samma säkerhetsåtgärd införs i ett eller flera styrdokument. Ett första styrdokument kan till exempel beskriva *att* säkerhetsåtgärden ska finnas, *var och när* den ska användas och *vem* som har ansvar för den. Ytterligare styrdokument på lägre nivåer i styrdokumentsstrukturen beskriver hur säkerhetsåtgärden anpassats till den nivå som krävs för säker informationsbehandling, (se **Använda Organisationens säkerhetsåtgärder**). I de flesta fall behövs fler än en nivå för att det ska vara möjligt att till slut förstå vem som behöver göra vad för att skyddet faktiskt ska fungera tillräckligt bra.

Innan du börjar arbetet med att föra in säkerhetsåtgärder i styrdokument behöver du tänka igenom hur du ska anpassa införandet till din organisations styrdokumentsstruktur (se **Utforma Styrdokument**). I denna vägledning utgår vi från en styrdokumentsstruktur i **två nivåer**:

- Riktlinje – organisationsövergripande regler
    - Instruktioner – regler som är specifika för en viss verksamhet, teknisk plattform eller situation

Använd begrepp och justera nivåerna till de som används i din organisation. Om tillgängliga nivåer och gängse uttryckssätt inte räcker till kan du behöva komplettera styrdokumenten med till exempel stöddokument eller utbildningar som förklarar det som inte blir tydligt i själva styrdokumenten.

Använd ett språk som organisationen är van vid när du skriver styrdokument. Om ord som har en viss betydelse inom informationssäkerhet har en annan betydelse i din organisation bör du justera språkbruket i så stor utsträckning som är möjligt till din organisations språkbruk. Undvik att använda samma ord med olika innebörd eller använda ett annat ord för samma innebörd som något som redan finns – det viktiga är att det blir tydligt vad som gäller.

Det är viktigt att tänka på att säkerhetsåtgärder är krav som organisationen ska uppfylla. Det behöver vara lätt att förstå hur en säkerhetsåtgärd ska efterlevas. Ta hjälp av till exempel existerande sammanställningar av rekommenderade säkerhetsåtgärder (best practice), exempelvis standarder på området, leta efter publicerade styrdokument från andra organisationer eller fråga kollegor i andra organisationer om du kan få tips på hur de gjort.

För att kunna arbeta med att anpassa säkerhetsåtgärderna behöver du ta reda på

- VAR den ska föras in (till exempel i nya eller befintliga styrdokument, om det behövs referenser m.m.)
- VEM som ansvarar för att den ger det skydd organisationen behöver (till exempel CISO, it-chef, HR, informationsägare)
- HUR den ska anpassas för att fungera i organisationen (dvs. till vilken nivå behöver den beskrivas i styrdokument för att få effekt och vilka förutsättningar krävs – behövs särskild kompetens, tillgång till särskilda verktyg etc.).

De säkerhetsåtgärder ni behöver införa kan vara beskrivna med olika detaljeringsgrad. Några kanske ligger på riktlinjenivå, medan andra delvis kan vara beskrivna hela vägen ner till instruktionsnivå. Ta hänsyn till detta när du planerar för var och hur säkerhetsåtgärden ska föras in i styrdokument.

1.1.4.4 Utforma organisationens arbete med säkerhetsåtgärder för styrning

Detta arbete går ut på att införa och förvalta organisationens systematiska informationssäkerhetsarbete i vissa organisationer också kallat ledningssystem för informationssäkerhet. Du kan läsa mer om detta i **Om metodstödet**. Här behöver arbetet integreras i organisationens befintliga sätt att leda och styra samt dess generella arbete med verksamhetsutveckling och verksamhetsarkitektur (se **Utforma Ledning och styrning**). Det är

också bra att säkerställa att relevanta nyckelroller blir engagerade i arbetet på olika områden (se **Nyckelroller inom informationssäkerhet**).

I din roll som CISO ingår att ha rollen som ansvarig för dessa säkerhetsåtgärder om du inte har en chef som har det formella ansvaret och du har delegerats uppgiften att få dem på plats.

1.1.4.4.1 Årshjul för dig som CISO

I takt med att ert systematiska arbete utvecklas behöver du som CISO skapa dig en översikt över när på året olika aktiviteter relaterade till organisationens ledning och styrning sker. Om till exempel handlingsplaner bör fastslås i samband med organisationens övergripande verksamhetsplanering behöver du börja med gapanalysen i tid för att hinna bli klar med dina prioriteringar för nästkommande år. Om andra ledningssystem rapporterar årlig uppföljning till ledningen, ledningens genomgång, i mars bör du sannolikt planera att göra detsamma.

I ditt årshjul behöver det också finnas plats för att följa upp och förbättra införda säkerhetsåtgärder för styrning, det vill säga att följa upp ditt eget arbete.

Den kanske viktigaste åtgärden i ditt årshjul är ledningens genomgång (se **Utforma Ledning och styrning** samt **Följa upp och förbättra Ledningens genomgång**). Planera så att du får in underlag som visar hur säkerheten ser ut från andra ansvariga i god tid för att kunna sammanställa och presentera resultatet för ledningen i rätt tid.

1.1.4.4.2 Dokumentation

En viktig del i CISO:s arbete är att hålla reda på allt som sker i relation till informationssäkerhetsarbetet. Du behöver därför utforma ett sätt att dokumentera ditt arbete. Dels behöver du dokumentera det du själv gör – dina egna instruktioner och arbetssätt. Dels behöver du sammanställa din och andras uppföljning samt andra relevanta säkerhetsrelaterade aktiviteter som sker i hela organisationen.

Sådant som tenderar att spreta, och därför är extra bra att börja dokumentera tidigt, är

- vilka styrdokument som innehåller vilka säkerhetsåtgärder
- vilka verksamhetsplaner som innehåller vilka informationssäkerhetsaktiviteter (se **Utforma Handlingsplan**)
- vem som har ansvar för att genomföra respektive följa upp säkerhetsåtgärder och eventuellt andra informationssäkerhetsaktiviteter
- när du ska följa upp säkerhetsåtgärder och informationssäkerhetsaktiviteter
- hur olika verksamheter arbetar med säkerhetsåtgärder och informationssäkerhetsaktiviteter utifrån styrningen.

Låt hellre dokumentationen vara levande, både till utformning och innehåll, än att vänta tills du har den perfekta mallen att dokumentera allt i. Börja dokumentera utifrån det behov du ser och utöka när du ser nya behov.

1.1.4.4.3 Bevaka förändringar som påverkar säkerhetsåtgärder för styrning

En del av det dagliga arbetet handlar om att löpande bevaka förändringar i omvärlden och i organisationen för att kunna justera styrning och stöd när det behövs. Sätt upp arbetssätt för att bevaka förändringar i omvärlden och i verksamheten (se **Identifiera och analysera: Omvärldsanalys** och **Verksamhetsanalys**). Förändringar som påverkar säkerhetsåtgärder för styrning är långsamma förändringar, men som ofta blir synliga tidigt i omvärldsbevakningen

och som ibland kräver omfattande åtgärder i styrningen av informationssäkerhet och för organisationen.

Håll särskilt utkik efter till exempel ändrade regleringar som påverkar ert informationssäkerhetsarbete eller er information, andra förändringar i krav och nya hot eller sårbarheter som kan påverka er organisation. Tänk också på sådant som förändras i organisationen – ansvar och roller som omdefinieras, tillkommande verksamheter, verksamheter som läggs ner eller större utkontrakteringar.

1.1.4.4.4 Förutsättningar för att utforma säkerhetsåtgärder för styrning

Tänk igenom hur arbetet med säkerhetsåtgärder för styrning ska genomföras, vilka roller som behövs (se **Utforma Organisation**), hur många anställda och hur mycket tid som kommer att gå åt för att möta ledningens mål (se **Utforma Informationssäkerhetsmål**).

Ta fram arbetssätt som hjälper dig att kontrollera hur väl styrningen fungerar. Prova säkerhetsåtgärder som ska användas ute i organisationen i begränsad omfattning först för att kunna justera dem så de fungerar bättre innan de beslutas och införs fullt ut (se **Utforma Riskhantering, Klassningsmodell, Kontinuitetshantering, Incidenthantering**).

Du behöver också ta fram en struktur för det du tar fram, så att de som ska använda styrningen lätt kan hitta och använda vad de behöver (se **Använda Riskanalys, Klassning av information, Genomföra och efterleva**). Det hjälper dig när du ska införa dina säkerhetsåtgärder. Kommer du själv behöva lägga mycket tid på införandet eller kan du utbilda personer som hjälper och avlastar dig?

Formulera målbilden för hur du ska sammanställa och presentera uppföljningen av dina säkerhetsåtgärder så att du kan visa på deras lämplighet, tillräcklighet och verkan (se **Följa upp och förbättra Utvärdera och följa upp**). Det hjälper dig när du utformar den uppföljning du behöver av olika säkerhetsåtgärder för att kunna svara på hur väl skyddad informationen i er organisation är. (ledningens genomgång).

1.1.4.5 Utforma organisationens arbete med säkerhetsåtgärder för informationsbehandling

Detta arbete går ut på att skapa den röda tråden mellan det systematiska informationssäkerhetsarbetet (som svarar på vilka säkerhetsåtgärder som behövs) och införandet av själva säkerhetsåtgärden (som skyddar informationen).

1.1.4.5.1 Säkerställ resurser utifrån behov i handlingsplaner

För att kunna arbeta med handlingsplaner (se **Utforma Handlingsplan**) för aktiviteter som inför eller förbättrar säkerhetsåtgärder behöver det finnas arbetssätt för att säkerställa resurser och följa upp att arbetet med säkerhetsåtgärder fortskrider enligt plan oavsett var i organisationen arbetet med åtgärden utförs.

Skyddet för informationen uppstår först när säkerhetsåtgärden är införd och fungerar väl i sin helhet. Alla steg fram till dess syftar till att uppnå just det och det är därför viktigt att fullfölja hela införandet (se **Använda Organisationens säkerhetsåtgärder**). Ta därför med hela kedjan i beräkningen när du estimerar hur mycket resurser som behövs för att införa eller förbättra en säkerhetsåtgärd. Planera tid och resurser på en tillräckligt detaljerad nivå för att införa en säkerhetsåtgärd fullt ut. Ibland är det flera säkerhetsåtgärder i kombination som införs och det kan bli svårt att estimera med någon större träffsäkerhet, gör ändå en bedömning av vad du tror.

1.1.4.5.2 Skapa förutsättningar för uppföljning

Den som är ansvarig för en säkerhetsåtgärd anpassar den genom att formulera de riktlinjer, instruktioner och annat stödmaterial som behövs. När detta genomförs och hur det ska följas upp styrs av handlingsplanerna (se **Utforma Handlingsplan**) och krav kopplat till hur ni ska följa upp i olika säkerhetsåtgärder (se **Följa upp och förbättra Utvärdera och följa upp**.)

Du som CISO stöttar organisationen i arbetet för att skapa bästa möjliga förutsättningar för att säkerhetsåtgärden ska fungera väl, och kunna följas upp. Ibland behöver uppföljningen kompletteras med någon ytterligare kontroll att kunna visa ledningen att den stämmer. Du bör därför i vissa fall planera för att kunna göra stickprov för att verifiera att det underlag du har fått är korrekt.

Det kan vara värdefullt att någon gång följa en säkerhetsåtgärd hela vägen från styrande dokument till införd och fungerande säkerhetsåtgärd som en del av din uppföljning. Det kan ge mycket information om organisationens informationssäkerhetsarbete och ge stöd till ansvariga med att förbättra säkerhetsåtgärden där du ser brister. Du får också ökad förståelse för olika säkerhetsåtgärder och hur de fungerar i din organisation.

1.1.4.5.3 Planera för styrdokument

Eftersom de flesta organisationer styrs genom styrdokument är utgångspunkten inom det systematiska informationssäkerhetsarbetet att varje säkerhetsåtgärd startar i ett sådant. Ofta införs en säkerhetsåtgärd på flera nivåer – med ökande detaljeringsgrad – innan den till slut är fullt införd. Säkerhetsåtgärden behöver anpassas för att fungera väl på alla nivåer för att kunna säkerställa att slutresultatet ger rätt skydd. Arbetet kan lätt bli omfattande, arbeta därför för att minimera komplexiteten och göra det enkelt för mottagarna att hitta rätt information och förstå vad de behöver göra.

Börja därför arbetet med att anpassa säkerhetsåtgärderna genom att ta fram en plan för var säkerhetsåtgärderna ska dokumenteras på högsta nivån och se till att alla nivåer därunder refererar uppåt.

Som CISO behöver du åtminstone hålla reda på vilka styrdokument på riktlinjenivå som innehåller säkerhetsåtgärder. På så sätt får du överblick över hur långt ni kommit i arbetet och har en startpunkt för när du behöver ta reda på vad som tagits fram på mer detaljerad nivå. Det kan också vara bra att sammanställa en lista med referenser till dokument på lägre nivåer. Det hjälper dig att hålla reda på status för olika aktiviteter i Organisationens handlingsplan för informationssäkerhet (se **Utforma Handlingsplan**) eller som är införda och följs upp enligt en årscykel.

1.1.5 Utbildning och kommunikation

Det är viktigt att tydligt kommunicera till berörda roller hur ni arbetar med säkerhetsåtgärder, inklusive ansvar, roller, uppföljning och övrigt stöd samt eventuella verktyg som ska användas.

Ni behöver analysera utbildningsbehovet kopplat till säkerhetsåtgärder och lägga in dem i organisationens utbildnings- och kommunikationsplan för informationssäkerhet (se **Använda Utbilda och kommunicera**). Vilka grupper som behöver veta vad gällande olika säkerhetsåtgärder analyserar du tillsammans med den som ansvarar för säkerhetsåtgärden.