

Stödmaterial om säkerhetsskydd

Kontroll av säkerhetsskydd



Innehåll

Inledning	3
1 Kravet på kontroll av säkerhetsskydd	4
1.1 Säkerhetsskyddslagstiftningen	4
1.2 Ledningens och säkerhetsskyddschefens ansvar för kontroll av säkerhetsskyddet	5
2 Kontroll av säkerhetsskydd.....	6
2.1 Planering	6
2.1.1 Utgå ifrån befintligt material och rutiner	6
2.1.2 Prioritera och välj inriktning	7
2.2 Genomför kontrollen.....	8
2.2.1 Kommunikation	8
2.2.2 Upplägg och metod	8
2.2.3 Sammanställa och bedöma underlag	10
2.3 Dokumentera resultatet av kontrollen	11
2.3.1 Rapport med identifierade avvikelser och när de ska vara åtgärdade.....	11
2.3.2 Återkoppling och dialog	11
2.3.3 Åtgärdsplan	11
2.3.4 Säkerhetsskyddsanalys och säkerhetsskyddsplan	11
2.4 Ta tillvara på erfarenheter från kontrollen.....	12

Inledning

Bakgrund

Det är av stor vikt för Sveriges säkerhet att verksamhetsutövare som bedriver säkerhetskänslig verksamhet har ett fullgott säkerhetsskydd. Verksamhetsutövaren ansvarar för sitt eget säkerhetsskydd och ska se till att regelverken följs. För att säkerställa detta krävs ett prioriterat och systematiskt säkerhetsskyddsarbete i organisationen. Ett viktigt verktyg för att säkerställa ett fullgott säkerhetsskydd är regelbunden uppföljning och kontroll. Genom att kontrollera säkerhetsskyddet kan verksamhetsutövaren identifiera sårbarheter och avvikelser i säkerhetsskyddet och vidta åtgärder för att säkerställa att den säkerhetskänsliga verksamheten har ett adekvat skydd.

Syfte

Detta material syftar till att fungera som ett stöd i arbetet med kontroll av säkerhetsskydd för verksamhetsutövare som tillämpar 2 kap. 14 § PMFS 2022:1. Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1) om kontroll och uppföljning av säkerhetsskyddet.

Stödmaterialet berör inte kontrollen av att en motpart följer kraven i ett säkerhetsskyddsavtal enligt 4 kap. 5 § första stycket säkerhetsskyddslagen 2018:585 och 7 kap. 8 § PMFS 2022:1.

Underlag

Stödmaterialet grundas på:

- kraven på kontroll enligt säkerhetsskyddslagstiftningen,
- erfarenheter och exempel från säkerhetsskyddschefer och
- kravet på att resultatet av kontrollen ska dokumenteras.

Läsaren rekommenderas även att ta del av Säkerhetspolisens vägledningar om säkerhetsskydd för exempel på vad kontroller kan omfatta.

Stödmaterialets upplägg

Stödmaterialet består av två delar.

I kapitel 1 beskrivs kravet på kontroll av säkerhetsskydd enligt säkerhetsskyddslagstiftningen och vilket ansvar den högsta ledningen respektive säkerhetsskyddschefen har för kontroller av den säkerhetskänsliga verksamheten.

I kapitel 2 presenteras exempel för planering av kontroller, genomförandet och hur resultaten från kontrollen kan användas. Avsnittet avslutas med hur erfarenheter från kontroller kan tas tillvara.

1 Kravet på kontroll av säkerhetsskydd

1.1 Säkerhetsskyddslagstiftningen

Det är viktigt att säkerhetsskyddsarbetet följs upp och utvecklas vid behov. Därför behöver en verksamhetsutövare utvärdera om säkerhetsskyddsåtgärderna ger effekt och kontrollera att verksamheten följer regelverket för säkerhetsskydd. Detta arbete kan göras på flera olika sätt, men ett grundläggande krav är att arbetet

genomförs systematiskt. Det innebär att verksamhetsutövaren behöver planera kontrollarbetet samt att kontroller sker regelbundet och dokumenteras. Att verksamhetsutövaren och säkerhetsskyddschefen ska kontrollera säkerhetsskyddet i den egna verksamheten regleras i säkerhetsskyddslagen och PMFS 2022:1.

Säkerhetsskyddslagen (2018:585)

2 kap. 1 § tredje stycket

Verksamhetsutövaren ska även kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta de åtgärder som krävs enligt denna lag.

2 kap. 7 § andra stycket

Säkerhetsskyddschefen ska leda och samordna säkerhetsskyddsarbetet samt kontrollera att verksamheten bedrivs enligt lagen och de föreskrifter som har meddelats i anslutning till lagen. Detta ansvar kan inte delegeras.

7 kap. 1 § andra punkten

Tillsynsmyndigheten får besluta att ta ut en sanktionsavgift av en verksamhetsutövare som inte har kontrollerat säkerhetsskyddet i den egna verksamheten enligt 2 kap. 1 § tredje stycket eller föreskrifter som har meddelats i anslutning till den bestämmelsen.

Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)

1 kap. 4 §

Bedömningar, beslut, planer och åtgärder samt uppföljning enligt föreskrifterna ska dokumenteras.

2 kap. 14 §

Verksamhetsutövaren ska systematiskt

1. utvärdera om säkerhetsskyddsåtgärderna ger avsedd effekt
2. identifiera brister och sårbarheter i säkerhetsskyddet, och
3. i övrigt kontrollera och följa upp att verksamheten följer regelverket för säkerhetsskydd.

Verksamhetsutövaren ska i en åtgärdsplan redovisa de åtgärder som behövs för att omhänderta avvikelser. I planen ska det anges vilken funktion som ansvarar för åtgärderna. Planen ska uppdateras löpande.

1.2 Ledningens och säkerhetsskyddschefens ansvar för kontroll av säkerhetsskyddet

Verksamhetsutövaren och säkerhetsskyddschefen har i säkerhetsskyddslagstiftningen ett utpekat ansvar för kontrollen av säkerhetsskyddet. För att kunna genomföra effektiva och adekvata kontroller av säkerhetsskyddet bör ledningen och säkerhetsskyddschefen

kontinuerligt överväga vilka kontroller som ska ske och hur dessa ska genomföras.

Nedan finns en checklista på frågor som ledningen och säkerhetsskyddschefen kan ställa sig i arbetet med kontroller av säkerhetsskyddet.

Ledningens ansvar

Ledningen är ytterst ansvarig för att säkerhetsskyddslagstiftningen efterlevs. Ledningen är även ansvarig för budget- och resursfrågor och har därmed en central roll i att skapa goda förutsättningar för säkerhetsskyddschefens arbete. Säkerhetsskyddsfrågor behöver därför diskuteras kontinuerligt och ett sätt för ledningen att följa upp säkerhetsskyddsarbetet och hur det kontrolleras kan exempelvis vara att diskutera följande frågeställningar:

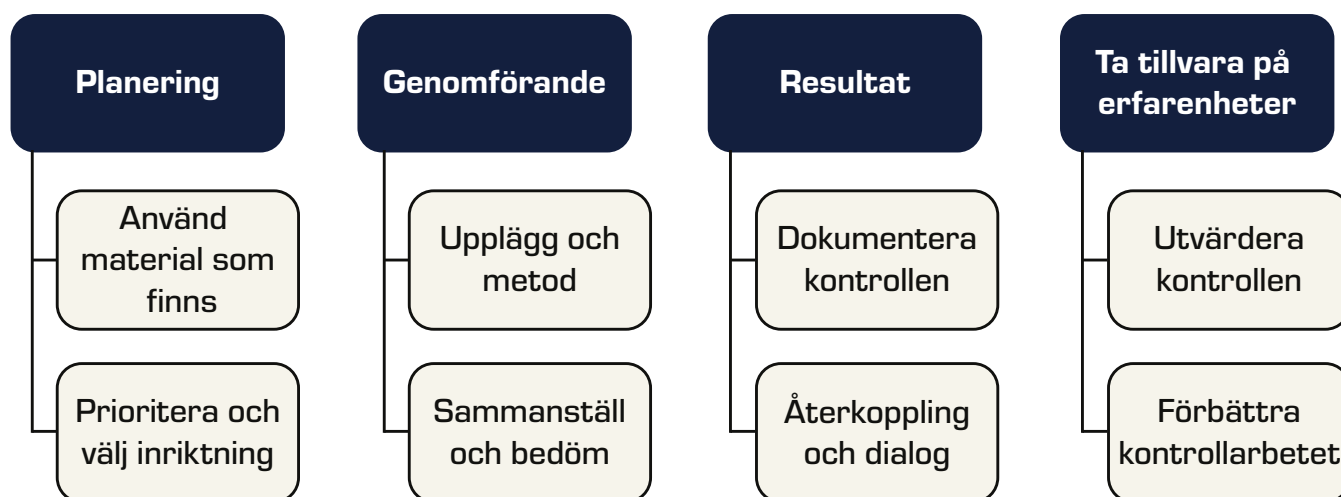
- Om ledningen har kännedom om verksamhetens säkerhetsskyddsanalys.
- Om ledningen har kunskap om och förståelse för verksamhetens skyddsvärden, hoten mot den säkerhetskänsliga verksamheten och verksamhetens sårbarheter.
- Om organisationens chefer har kännedom om vilka åtgärder som ska vidtas i deras verksamhetsdel om en sårbarhet i säkerhetsskyddet upptäcks.
- Om det finns interna föreskrifter avseende säkerhetsskydd som är aktuella och tillämpas.
- Om säkerhetsskyddschefen har förutsättningar för att uppfylla det som åligger funktionen enligt säkerhetsskyddslagen.
- Om ledningen har kännedom om hur verksamhetens säkerhetsskyddsarbete kontrolleras.
- Om det finns en plan för när under verksamhetsåret kontroller ska utföras och på vilket sätt.
- Om ledningen har kännedom om resultatet av genomförda kontroller.

Säkerhetsskyddschefens ansvar

Säkerhetsskyddschefen ska leda och samordna säkerhetsskyddsarbetet samt kontrollera att verksamheten bedrivs enligt lagen. Frågor för säkerhetsskyddschefen att ställa sig inför planering av kontroll av säkerhetsskyddet kan till exempel vara:

- Om interna föreskrifter reglerar vem som ansvarar för vad avseende säkerhetsskydd.
- Om interna föreskrifter är implementerade och efterlevs.
- När under verksamhetsåret kontroller ska utföras och om de behöver förankras med ledningen.
- Vilket sätt kontrollerna ska genomföras på.
- Om rapporteringsvägar är förankrade i organisationen när en sårbarhet upptäcks.
- Om säkerhetsskyddschefen får rapporter om säkerhetshotande händelser och sårbarheter i säkerhetsskyddet.
- Om medarbetarna har den förståelse de behöver om verksamhetens skyddsvärden och hotet gentemot dessa.
- Om medarbetarna har den förståelse de behöver för de planerade säkerhetsskyddsåtgärder som ska vidtas.

2 Kontroll av säkerhetsskydd



Kontroll av säkerhetsskyddsarbetet kan genomföras på många olika sätt. Ovan presenteras ett ramverk för hur en verksamhet kan gå till väga i kontrollen av säkerhetsskyddsarbetet.

2.1 Planering

Verksamhetsutövare bör i planeringsstadiet lägga grunden för ett tillvägagångssätt som kan identifiera brister och sårbarheter i säkerhetsskyddet. Vid planeringen av kontrollerna kan verksamhetsutövaren med fördel utgå från redan befintliga tillvägagångssätt som finns för kontroll av den specifika verksamheten. Det är även viktigt för verksamhetsutövaren att prioritera vad som ska kontrolleras.

2.1.1 Utgå ifrån befintligt material och rutiner

Ett första steg för att avgöra vilka kontroller som ska genomföras är att undersöka vilken typ av relevanta planer, beslut och övrig information om säkerhetsskyddet som redan finns inom organisationen utöver säkerhetsskyddsanalysen och säkerhetsskyddsplanen. Exempelvis kan den som utför kontrollen utgå från framtagna rutiner och stöddokument kopplat till säkerhetsskyddslagstiftningen.

Utöver säkerhetsskyddslagstiftningen finns flera andra regelverk som ställer krav på kontroll och att verksamhet ska bedrivas enligt gällande rätt. En verksamhetsutövare kan undersöka vilka regelverk med sådana krav som de träffas av och hur de eventuellt liknar eller skiljer sig åt. Regelverkens likheter i kraven på kontroll medför att vissa förfaranden kan komma att likna varandra. Kraven i andra regelverk kan komma att skilja sig åt och behöver då omhändertas och kontrolleras var för sig. Säkerhetsskyddsarbetet kan i praktiken ha beröringspunkter med arbete som görs i andra delar av organisationen, som till exempel analysarbete, incidenthantering och säkerhetsåtgärder. Genom att samordna arbetet med olika processer internt kan arbetsbelastning och risken för dubbelarbete minska.

Notera:

Personer som arbetar med kontroller av säkerhetsskydd behöver vara behöriga att ta del av den information som kontrollen omfattar. Detta behöver beaktas vid eventuella samarbeten med andra inom organisationen.

Exempel på andra regelverk och processer som kan ha beröringspunkter med kontroll av säkerhetsskydd

Inköp och upphandling	Personalsäkerhet/HR	Diarietförelägg och posthantering
Internrevision	Intern styrning och kontroll	Informationssäkerhet och it-säkerhet
Personuppgiftshantering	Fastighet/fysisk säkerhet	Arkiv
Beredskapsarbete	Utveckling av it-system/Inköp it-system	Utlämnande av allmän handling/ sekretess/ säkerhetsskyddsklassificering
Arbetsmiljö	Utbildningsverksamhet	Medarbetarundersökningar

2.1.2 Prioritera och välj inriktning

Det går inte att kontrollera hela verksamheten eller alla bestämmelser samtidigt. För att avgöra vad som ska kontrolleras är det fördelaktigt att först göra ett urval för att sedan ta fram en plan för när och hur kontroller ska genomföras. Vissa verksamhetsutövare kallar detta för kontrollplan.

En kontrollplan kan inbegripa vilka delar av verksamheten som ska kontrolleras, vilket sätt kontrollerna ska göras på och vilka bestämmelser som ska omfattas. En variation i urvalen kan skapa en bredd i kontrollverksamheten och ge en mer heltäckande bild av säkerhetsskyddets ändamålsenlighet. Tänk på att vissa kontroller regleras i säkerhetsskydds-

lagstiftningen och därmed alltid ska genomföras, exempelvis säkerhetsloggning och säkerhetsövervakning enligt 4 kap. 25–31 §§ PMFS 2022:1.

En organisations verksamhetsgrenar skiljer sig åt både till innehåll och komplexitet vilket innebär att kontrollen bör utformas utifrån den specifika verksamhetsdelen. Säkerhetsskyddslagstiftningen ska följas men tillvägagångssättet kan se olika ut.

Inom en verksamhet kan det framkomma uppgifter om misstänkta eller konstaterade sårbarheter i säkerhetsskyddet som tidigare varit okända. När sådana situationer uppstår är det viktigt att bedöma om händelsestyrda kontroller behöver prioriteras framför det planerade arbetet.

Exempel på urval för inriktning av kontrollen

- Områden som rör bestämmelser som det har rapporterats säkerhetshotande händelser eller incidenter om.
- Områden som rör bestämmelser för de högsta skyddsvärdena.
- En enskild bestämmelse som kontrolleras i alla delar av verksamheten som bedriver säkerhetskänslig verksamhet.
- Dokumenterade beslut och rutiner som ska finnas enligt säkerhetsskyddslagstiftningen.
- Teman (fysisk säkerhet, informationssäkerhet och personalsäkerhet).

2.2 Genomför kontrollen

2.2.1 Kommunikation

För att uppnå önskvärd effekt av kontrollen är det viktigt med en god kommunikation mellan alla berörda delar i verksamheten. Att exempelvis informera den berörda verksamhetsdelen och ledningen om att en kontroll initieras ger verksamhetsutövaren en möjlighet att förbereda sig. Det kan till exempel handla om att ha relevant dokumentation tillgänglig för granskning och rätt personal på plats vid tillfället för kontrollen. Att upprätthålla en bra kommunikation under kontrollen kan öka förtroendet och förväntansbilden från både ledningen och den berörda verksamhetsdelen och därmed minska risken för missförstånd. Att kommunicera resultatet efter genomförd kontroll möjliggör att resultatet av kontrollen kan förankras bättre i organisationen.

2.2.2 Upplägg och metod

Det finns många olika sätt att systematisera och genomföra kontrollen. Gemensamt för samtliga kontroller är att någon form av information eller data behöver samlas in, sammanställas, analyseras och bedömas.

Kontroller innehåller många dimensioner. De kan fokusera ensidigt på exempelvis regelefterlevnad men även på kvalitet. Kontroller kan även omfatta enskilda eller flera bestämmelser i regelverket. Hur en kontroll genomförs kan alltså variera och det är därför särskilt viktigt att fundera över vad syftet med kontrollen är och anpassa upplägget efter det.

Nedan ges några exempel på olika typer av metoder för att genomföra en kontroll.

En praktisk kontroll av den säkerhetskänsliga verksamheten innebär att en verksamhet testar säkerhetsskyddet.

Ett praktiskt test kan vara att genomföra penetrationstester för att säkerställa att säkerhetskraven som finns på informations-system som är av betydelse för Sveriges säkerhet efterlevs.

Vidare kan en verksamhet utföra praktiska tester på verksamhetens fysiska skydd. Exempel kan vara att testa lås, larm och passersystem eller att kontrollera att verksamheten efterlever kraven som finns i beskrivningen av dimensionerande antagonistiska förmågor (DAF), om verksamheten har blivit tilldelad en sådan.

En automatisk kontroll kan vara inbyggd i verksamhetsutövarens processer, system och rutiner.

Ett exempel på en automatisk kontroll kan vara att använda ett diarieföringssystem som inte möjliggör att en handling diarieförs om den inte har en anteckning om säkerhetsskyddsklass. Viktigt att tänka på är att denna typ av kontroll inte reglerar om uppgifter delas in i adekvat säkerhetsskyddsklass. Det säkerställer inte heller att alla säkerhetsskyddsklassificerade handlingar endast finns i system som är anpassade för säkerhetsskyddsklassificerade uppgifter. Ett möjligt sätt att fånga den typen av aspekter är att använda sig av stickprov där verksamhetsutövaren kontrollerar ett antal handlingar för att bedöma om de har en adekvat anteckning om säkerhetsskyddsklass. Ett sådant stickprov kan ge en indikation eller se om det finns behov av att genomföra

utbildningsinsatser avseende hur verksamheten delar in säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass och förser handlingar med anteckning om säkerhetsskyddsklass.

Ett annat exempel är att en verksamhetsutövare skapar digitala utbildningar som anställda måste genomföra samt bli godkända på för att kunna delta i säkerhetskänslig verksamhet. Sådana utbildningar kan exempelvis rikta sig till anställda som ska använda en bärbar dator som kan hantera säkerhetsskyddsklassificerade uppgifter, få tillgång till informationssystem som är av betydelse för Sveriges säkerhet eller som ska fatta beslut utifrån kraven i säkerhetsskyddslagstiftningen. En verksamhetsutövare kan genom sådana automatiserade utbildningskontroller öka möjligheten till att anställda är medvetna om vilka krav som följer av säkerhetsskyddslagstiftningen. Automatiserade utbildningskrav säkerställer dock inte att alla anställda som har tillgång till en bärbar dator som kan hantera säkerhetsskyddsklassificerade uppgifter har kännedom om samtliga krav. Det kan därför vara nödvändigt att genomföra uppföljande utbildningsinsatser.

Vidare kan en verksamhetsutövare använda sig av system som medför att det kontinuerligt sker kontroller av det fysiska säkerhetsskyddet.

Exempel på sådan åtgärd är att använda sig av ett inpasseringssystem som kräver att personalen använder sig av både passerkort och kod för att kunna få tillgång till den säkerhetskänsliga verksamheten.

En förenklad kontroll kan vara att en verksamhetsutövare skickar ut en blankett till medarbetare som arbetar i den säkerhetskänsliga verksamheten.

Exempel på en sådan självskattningsblankett är att verksamhetsutövaren skickar ut en lista där enskilda bestämmelser beskrivs och där regelefterlevnad av respektive bestämmelse bekräftas med signatur och datum. Protokollet återrapporteras till säkerhetsskyddschefen. Förfarandet kan även kombineras med en utbildningspresentation till chefer för att sprida kunskap om säkerhetsskydd i organisationen.

Det är viktigt att tänka på hur denna kontroll ska genomföras. Bedömningarna som görs i listan behöver vara underbyggda och ge en rättvisande bild av måluppfyllelsen.

Exempel på en förenklad kontroll

	Datum och signatur för bekräftelse
Säkerhetsskyddsklassificerade uppgifter behandlas endast i informationssystem eller lagringsmedium som är godkända för aktuell klass (3 kap. 1 § PMFS 2022:1).	
Lagringsmedier som innehåller uppgifter i säkerhetsskyddsklassen konfidentiell eller högre inventeras minst en gång per år (3 kap. 21 § PMFS 2022:1).	

En fördjupad kontroll med intervjuer kan utgöra ett bra komplement till skriftlig dokumentation eftersom de kan öka förståelsen för verksamheten och de bakomliggande orsaker till varför och när säkerhetsskydds-

arbetet är adekvat och inte. Kontrollens inriktning avgör vilka personer och funktioner som är aktuella att intervjua. Frågeunderlaget kan i vissa fall med fördel skickas ut till de berörda personerna innan intervjutillfället.

Exempel på fördjupad kontroll med intervjuer – kontrollera om säkerhetsskyddsklassificerade handlingar har en anteckning om säkerhetsskyddsklass

- Välj två avdelningar som hanterar säkerhetsskyddsklassificerade uppgifter i olika säkerhetsskyddsklasser.
- Ta fram intervjufrågor med utgångspunkt till verksamhetens rutiner för indelning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass och att förse säkerhetsskyddsklassificerade handlingar med anteckning om säkerhetsskyddsklass.
- Välj slumpmässigt ut handläggare och chefer på de två avdelningarna.
- Genomför först intervjuer med medarbetare för att sedan stämma av eventuella frågetecken med cheferna.
Fråga medarbetarna
 - hur de går tillväga för att bedöma om uppgifterna är säkerhetsskyddsklassificerade och i vilken säkerhetsskyddsklass
 - om de känner till rutinerna för indelning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass
 - om de anser att det fanns förbättringsbehov i utbildning eller systemstöd kopplat till hur indelningen ska gå till.
- Fråga cheferna
 - hur de säkerställer att medarbetare har den kompetens som krävs för att dela in en säkerhetsskyddsklassificerad uppgift i säkerhetsskyddsklass
 - hur de säkerställer att uppgifter indelas i adekvat säkerhetsskyddsklass.

2.2.3 Sammanställa och bedöma underlag

När informationsinhämtningen är klar behöver underlaget analyseras och bedömas utifrån de bestämmelser som kontrollen har utgått från. Det är bra att dokumentera tillvägagångssättet och resultatet av kontrollen i till exempel en rapport så att informationen sparas.

2.3 Dokumentera resultatet av kontrollen

Resultatet av kontrollarbetet kan tas om hand på olika sätt. Avvikelser och sårbarheter ska dokumenteras. Beroende på omfattning kan avvikelserna och sårbarheterna dokumenteras antingen i en åtgärdsplan eller i säkerhetsskyddsanalysen/säkerhetsskyddsplanen.

2.3.1 Rapport med identifierade avvikelser och när de ska vara åtgärdade

När kontrollen är utförd kan den funktion som genomfört kontrollen sammanställa och dokumentera resultatet i exempelvis en rapport. I den rapport som beskriver kontrollens resultat ska det tydliggöras vad som ska göras för att verksamheten ska leva upp till lagens krav eller vad som kan göras för att kvaliteten ska bli bättre. En annan viktig aspekt är att rapporten kan behöva rikta sig till flera funktioner inom verksamheten beroende på vem som har mandat att ändra eller vidta vissa kravställda åtgärder. Det är därför viktigt att föra en dialog med alla relevanta funktioner och tydligt redogöra vem som är ansvarig för att åtgärda vilken avvikelse.

Av rapporten bör det också framgå datum för när avvikelserna ska vara åtgärdade. Uppföljningstiden bör anpassas utifrån avvikelsernas art och omfattning. De eller den som rapporten riktar sig till bör redovisa hur varje avvikelse har åtgärdats.

2.3.2 Återkoppling och dialog

Om den som utför kontrollen direkt konstaterar akuta sårbarheter i säkerhetsskyddet kan dessa med fördel meddelas omedelbart och i anslutning till kontrolltillfället. Det ger verksamhetsutövaren möjlighet att tidigt påbörja arbetet med förbättringsåtgärder för avvikelser som kommer att nämnas i slutrapporten.

När det är dags att presentera rapporten med konstaterade avvikelser görs det med fördel muntligt. Detta för att säkerställa att de berörda har förstått de sårbarheter och avvikelser som presenteras. Tillfället ger även verksamheten möjlighet att ställa frågor och kan ses som en möjlighet att ge vägledning i säkerhetsskydd. Vid mötet kan det även ges exempel på hur andra delar av organisationen arbetar på det aktuella området.

2.3.3 Åtgärdsplan

Verksamhetsutövaren ska i en åtgärdsplan redovisa de åtgärder som behövs för att omhänderta avvikelser. I åtgärdsplanen ska det anges vilken funktion som ansvarar för åtgärderna. Det kan även vara fördelaktigt att i åtgärdsplanen dokumentera när avvikelserna ska vara åtgärdade.

Åtgärdsplanen är ett komplement till arbetet med säkerhetsskyddsanalysen och säkerhetsskyddsplanen. Syftet med åtgärdsplanen är att verka som ett dokument för systematiska och kontinuerliga kontroller, utan att säkerhetsskyddsanalysen och säkerhetsskyddsplanen ska behöva uppdateras och fastställas vid varje tillfälle en avvikelse eller sårbarhet identifieras.

2.3.4 Säkerhetsskyddsanalys och säkerhetsskyddsplan

Om kontrollen visar på omfattande avvikelser eller tidigare oidentifierade sårbarheter kan det finnas behov av att hantera dessa i säkerhetsskyddsanalysen och säkerhetsskyddsplanen. Detta innebär att verksamhetsutövaren behöver uppdatera och fastställa dokumenten på nytt (2 kap. 1 § säkerhetsskyddsförordningen 2021:955 och 2 kap. 10 och 12 §§ PMFS 2022:1). Exempel på när säkerhetsskyddsanalysen och säkerhetsskyddsplanen kan behöva uppdateras är när det finns behov av att planera och vidta nya eller ytterligare säkerhetsskyddsåtgärder.

En avvikelse eller en sårbarhet som snabbt går att åtgärda och som bedöms ha liten betydelse för säkerhetsskyddsåtgärdens sammantagna effekt behöver inte tillföras säkerhetsskyddsanalysen. Ett exempel på detta kan vara att justera i befintliga rutiner och göra mindre ändringar i beslutade säkerhetsskyddsåtgärder.

När säkerhetsskyddsanalysen och säkerhetsskyddsplanen ska uppdateras och fastställas bör de kvarstående sårbarheterna och säkerhetsskyddsåtgärderna som framgår av åtgärdsplanen tillföras dokumenten.

2.4 Ta tillvara på erfarenheter från kontrollen

Det är viktigt att utvärdera arbetet med kontroller. Det bör göras såväl i ledningen som av chefer och medarbetare. Utvärderingsfrågor kan exempelvis vara:

- Är ansvaret för kontroll av den säkerhets-känsliga verksamheten tydlig och känd hos verksamhetsutövaren?
- Genomförs kontroller av säkerhetsskyddet regelbundet i verksamheten?
- Leder kontrollerna till att nödvändiga åtgärder vidtas?
- Är de genomförda kontrollerna adekvat genomförda sett till den säkerhets-känsliga verksamhet som kontrolleras?
- Förbättrar kontrollerna säkerhetsskyddsarbetet?
- Har ledningen kunskap om arbetet med och resultatet av kontrollerna?
- Genomförs kontroller enligt kontrollplanen?
- Resulterar kontroller i åtgärder som omhändertar grundorsakerna till avvikelser?

Notera:

Det är alltid verksamhetsutövaren som ansvarar för sitt säkerhetsskydd och som ska säkerställa att säkerhetsskyddet är fullgott.

Olika verksamheter har olika förutsättningar för att genomföra kontroller av sitt säkerhetsskydd. Genom att utvärdera hur kontroller planerats, genomförts och återkopplats får verksamheter större möjlighet att utveckla kontrollformer som är anpassade efter verksamhetens specifika förutsättningar.



Säkerhetspolisen

Box 12312, 102 28 Stockholm
010-568 70 00 | sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se