EN GRANSKNINGSRAPPORT FRÅN RIKSREVISIONEN

TILL RIKSDAGEN

DATUM: 2016-05-04
DNR: 31-2014-1526
RIR 2016:8

Härmed överlämnas enligt 9 § lagen (2002:1022) om revision av statlig verksamhet m.m. följande granskningsrapport över effektivitetsrevisionen:

Informationssäkerhetsarbete på nio myndigheter

En andra granskning av informationssäkerhet i staten

Riksrevisionen har granskat hur följande myndigheter arbetar med sin informationssäkerhet: Arbetsförmedlingen, Affärsverket svenska kraftnät, Bolagsverket, Försäkringskassan, Lantmäteriet, Migrationsverket, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk. Regeringen, Regeringskansliet och Ekonomistyrningsverket har också ingått i granskningen. Resultatet av granskningen redovisas i denna granskningsrapport.

Företrädare för Regeringskansliet och de granskade myndigheterna har fått tillfälle att faktagranska och i övrigt lämna synpunkter på utkast till rapporten. Riksrevisionen vill tacka seminariedeltagare från Försvarshögskolan, Totalförsvarets forskningsinstitut, Örebro universitet, Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap, Arbetsförmedlingen, Försäkringskassan, Migrationsverket och Riksrevisionen för synpunkter. Riksrevisionen står dock helt för de slutsatser som dras i rapporten.

Rapporten innehåller slutsatser och rekommendationer som avser Regeringskansliet och de granskade myndigheterna. Utöver den tryckta versionen av granskningsrapporten omfattar detta beslut bilagorna 5 och 6 i elektronisk form, vilka framgår av innehållsförteckningen.

Riksrevisor Margareta Åberg har beslutat i detta ärende. Revisionsdirektör Per Dackenberg har varit föredragande. Enhetschef Jörgen Lindström och revisionsdirektör Marcus Pettersson har medverkat i den slutliga handläggningen.

Margareta Åberg

Per Dackenberg

För kännedom:
Regeringen, Justitiedepartementet, Affärsverket svenska kraftnät, Arbetsförmedlingen, Bolagsverket, Ekonomistyrningsverket, Försäkringskassan, Lantmäteriet, Migrationsverket, Post- och telestyrelsen, Sjöfartsverket, Statens tjänstepensionsverk

INFORMATIONSSÄKERHETSARBETE PÅ NIO MYNDIGHETER

RIKSREVISIONEN

Innehåll

Elektroniska bilagor

Till rapporten finns två ytterligare bilagor att ladda ned från Riksrevisionens webbplats www.riksrevisionen.se. Dessa kan begäras ut från ärendets akt genom registraturen.

Bilaga 5. Enkät till Affärsverket svenska kraftnät, Bolagsverket, Lantmäteriet, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk

Bilaga 6. Konsultrapport: Radar Ecosystem Specialists: IT- och informationssäkerhet – statliga myndigheter och verk, 2015–2016

Sammanfattning och slutsatser

I statsförvaltningen hanteras mycket information som är skyddsvärd. Informationssäkerhet innebär att se till att all skyddsvärd information är tillgänglig, riktig, konfidentiell och spårbar. Informationssäkerhet är en fråga som berör samtlig personal i en myndighet. Att skapa en god informationssäkerhet är viktigt eftersom brister i denna kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att utbetalningar av transfereringar stoppas.

I Riksrevisionens föregående granskning av informationssäkerheten i den civila statsförvaltningen från 2014 berördes ett antal hot och risker. Det handlar om att många samhällsfunktioner är beroende av informationsteknologi för att kunna fungera. Olika tekniska system är dessutom ofta beroende av varandra eller tekniskt sammankopplande, vilket utgör en sårbarhetsfaktor i sig genom att störningar kan få konsekvenser som både är svåra att förutse och hantera. Vad som utgör ett hot eller en risk varierar från exempelvis stater, statsunderstödda aktörer, terrorister och organiserad brottslighet till fel och störningar som inte orsakas av antagonister utan beror på mjuk- eller hårdvarufel, processbrister, bristande kvalitetskontroll, slarv, missbedömningar eller rena olycksfall. Vilka som drabbas kan vara allt från enskilda individer till hela samhällssektorer. Konsekvenserna kan till exempel vara uteblivna betalningar av transfereringar och störningar i el- eller vattenförsörjning.

Granskningens bakgrund

Riksrevisionen granskade under 2005–2007 arbetet med informationssäkerhet vid elva myndigheter i statsförvaltningen. Granskningarna visade ett flertal brister. Regeringen hade inte följt upp om myndigheternas interna styrning och kontroll av informationssäkerhet var tillfredsställande och inte heller gett myndigheterna tillräckliga förutsättningar för ett effektivt informationssäkerhetsarbete. Under 2014 granskade Riksrevisionen ånyo informationssäkerhet med inriktning mot regeringen och dess expertmyndigheters styrning och stöd. Denna granskning visade att det fanns påtagliga brister i arbetet med informationssäkerhet och att regeringen inte utövat en effektiv styrning.

Granskningens syfte

Syftet med denna granskning har varit att undersöka hur nio myndigheter arbetar med sin informationssäkerhet. Dessa myndigheter bedriver samhällsviktig verksamhet, hanterar mycket pengar, är starkt IT-beroende och hanterar skyddsvärd information. Riksrevisionen har granskat om myndigheterna utifrån dagens krav och förutsättningar bedriver ett informationssäkerhetsarbete så att de uppnår ett ändamålsenligt skydd av sina informationstillgångar. Ett annat syfte har varit att granska

om regeringen säkerställer att de granskade myndigheterna har en effektiv intern styrning och kontroll av sin informationssäkerhet.

För att informationssäkerheten ska vara effektiv, såväl för respektive myndighet som för statsförvaltningen i stort, krävs att det går att väga kostnader mot nytta. Därför har Riksrevisionen låtit undersöka kostnadsbilden för informationssäkerhetsarbete.

Granskningens resultat

Riksrevisionens slutsatser

Riksrevisionens samlade slutsats är att arbetet med informationssäkerhet på de granskade myndigheterna ligger på en nivå som är märkbart under vad som är tillräckligt. En viktig förklaring till det är att förståelsen för vikten av en god informationssäkerhet överlag är alltför liten. Detta får till följd att arbetet med informationssäkerhet inte blir tillräckligt högt prioriterat i förhållande till de risker som finns. Detta gäller såväl för regeringen, som borde kunnat vara tydligare med att styra myndigheterna i frågan som för myndigheternas ledningar, som inte prioriterat arbetet med informationssäkerhet i den utsträckning som krävs. Mycket tyder på att det är svårt för många myndigheter att få till stånd ett ändamålsenligt informationssäkerhetsarbete. Riksrevisionen har därför ingen anledning att anta att den bild som framträder vid de granskade myndigheterna inte skulle gälla även för flertalet andra myndigheter i statsförvaltningen.

Arbetet med informationssäkerhet når inte upp till en godtagbar nivå på de granskade myndigheterna

Granskningen av Arbetsförmedlingen, Försäkringskassan och Migrationsverket har varit särskilt djupgående. Ingen av dessa myndigheter kan sägas ha ett systematiskt informationssäkerhetsarbete som motsvarar kraven i Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter om statliga myndigheters informationssäkerhet. Dessa krav innebär att myndigheterna ska tillämpa ett ledningssystem som bland annat omfattar att de ska upprätta en policy för informationssäkerhet, klassificera sin information med utgångspunkt från riktighet, tillgänglighet och konfidentialitet samt utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur de ska hantera risker.

En viktig förutsättning för att lägga grunden till en god informationssäkerhetskultur och för att skapa förståelse för informationssäkerhet är att myndighetens ledning visar engagemang i frågan. Granskningen visar att myndigheternas ledningar har delegerat ansvaret för informationssäkerhet, utan att se till att de ansvariga har ett tillräckligt mandat att utföra sina uppgifter och tillräckligt med resurser. De funktioner som ansvarar för informationssäkerheten har svårt att hävda sig mot kärn-

verksamheten som tenderar att se kraven på informationssäkerhet som hinder, vilket får till följd att verksamhetens krav på funktionalitet mestadels går före kraven på säkerhet. Det är snarare IT- eller säkerhetsfunktionerna som ställer krav på säkerhet än kärnverksamheten. Situationen på de sex andra granskade myndigheterna – Affärsverket svenska kraftnät, Bolagsverket, Lantmäteriet, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk – varierar, men sammanfaller i stora delar med hur det ser ut på de tre särskilt djupt granskade myndigheterna.

Trots att myndigheterna har tagit fram policyer, riktlinjer och handledningar i fråga om informationssäkerhet är kännedomen om vad dessa dokument har för innehåll och syfte låg hos många medarbetare och chefer. Säkerhetsarbetet implementeras inte i de ordinarie verksamhetsprocesserna. Kärnverksamheten uppfattar inte att den har något ansvar för informationssäkerheten, utan att det ligger någon annanstans i myndigheten såsom på IT- eller säkerhetsfunktioner. Det saknas till betydande delar delaktighet och ansvarstagande som bör genomsyra hela myndigheten, och det finns en bristande förståelse för behovet av säkerhetsinvesteringar utan synbar nytta.

Riskanalyser sker på varierande sätt inom och mellan de granskade myndigheterna och omfattar mer än endast informationssäkerhet. Det är inte fel i sig, men inom myndigheterna bidrar det till överlappningar och risk för att områden hamnar mellan stolarna såväl som att vissa områden inte blir belysta. Myndigheterna sammanställer sällan sina olika analyser till en övergripande analys med inriktning mot informationssäkerhet. Sett från ett informationssäkerhetsperspektiv är det ett splittrat tillvägagångssätt, som behöver samordnas bättre.

Det är svårt att få en samlad bild av informationssäkerhetsläget vid myndigheterna, vilket hänger samman med att det ofta saknas en strukturerad uppföljning av hur ledningssystemet fungerar. Bristen på uppföljning försvårar ett förbättringsinriktat arbetssätt. Avsaknaden av ett lärandeperspektiv visar sig även i incidenthanteringen, som mer är inriktad mot att skapa statistik än att ta reda på orsaker till att incidenter inträffar.

Riksrevisionen kan konstatera att arbetet med informationssäkerhet på de granskade myndigheterna sker på varierande sätt, trots att betydande delar av detta arbete borde vara generiskt till sin karaktär. Det kan också konstateras att de delar av informationssäkerhetsarbetet som omfattar IT-säkerhet och fysiskt skalskydd överlag visar sig bättre än de organisatoriska delarna, även om det för IT-säkerhet finns förbättringspotential. Många av komponenterna i ledningssystemet verkar finnas till för att det är ett krav, snarare än att de skulle kunna vara ett kraftfullt verktyg för att bedriva förändringsarbete.

Regeringen har inte sett till att det finns nödvändiga förutsättningar

Vid en första anblick kan förutsättningarna synas vara till fyllest genom att regeringen har skapat vissa förutsättningar för myndigheterna att kunna arbeta med intern styrning och kontroll av informationssäkerheten. Det finns en struktur på plats med olika författningar som är avsedda att styra detta arbete. En del i detta är att regeringen har beslutat att ledningen för ett antal myndigheter ska intyga att den interna styrningen och kontrollen är betryggande. Varje departement för dessutom regelbundna dialoger med myndigheternas ledning. Likväl visar granskningen att det är allvarliga brister i myndigheternas informationssäkerhetsarbete.

Riksrevisionen bedömer att det behövs en starkare styrning från regeringen gentemot myndigheterna, så att nödvändiga säkerhetsåtgärder verkligen blir genomförda. Att enbart ta fram ett övergripande regelverk är inte tillräckligt för att säkerheten ska bli god. Om regeringen inte efterfrågar information om myndigheternas informationssäkerhet och inte framhåller vikten av god informationssäkerhet bedömer Riksrevisionen att myndigheternas ledningar inte heller kommer att prioritera frågan.

Kostnaderna för informationssäkerhet är okända

För att kunna ta ställning till om det fattas välgrundade beslut om vilka åtgärder som behöver vidtas för att skydda all information i statsförvaltningen som är värd att skydda behövs en samlad lägesbild över hot, risker och lämpliga åtgärder. Till detta kommer ett behov av att känna till hur stora kostnader som årligen läggs ned på informationssäkerhet. Först när dessa bilder har framträtt är det möjligt att väga kostnader mot nytta av skyddsåtgärder och på så sätt uppnå en optimal nivå på informationssäkerheten i staten som helhet.

Det saknas i dag uppgifter om myndigheternas kostnader för informationssäkerhet, såväl när det gäller enskilda myndigheter som för statsförvaltningen i stort. Därmed går det inte att uttala sig om hanteringen av informationssäkerheten är kostnadseffektiv. Det är enligt Riksrevisionens bedömning en påtaglig brist att regeringen inte efterfrågar dessa uppgifter, särskilt i förhållande till att IT är utpekat som ett centralt verktyg för att utveckla statsförvaltningen.

Resurserna används sannolikt inte effektivt

Den svenska statsförvaltningen fungerar på det sättet att myndigheterna åtnjuter en långtgående självständighet när det gäller att organisera sin verksamhet. Av det följer att alla myndigheter i statsförvaltningen, oavsett storlek, har att själva ombesörja sin egen informationssäkerhet. Det innebär att de antingen måste göra det mesta av arbetet själva, eller anlita konsulter. För de största myndigheterna är förutsättningarna bättre för att på egen hand kunna bygga upp och upprätthålla en god informationssäkerhet på grund av skalfördelar. För de flesta av myndigheterna är dock förutsättningarna inte lika goda. Denna granskning har visat att det är en tung

uppgift även för tämligen stora myndigheter att bedriva ett framgångsrikt informationssäkerhetsarbete. MSB bistår med bra vägledning för hur en myndighet ska arbeta med informationssäkerhet. För flera av de granskade myndigheterna är det likväl inte tillräckligt då de faktiskt lider brist på operativt bistånd, något som MSB inte lämnar i dag. Detta leder enligt Riksrevisionens bedömning till att informationssäkerhetsarbetet på aggregerad nivå sannolikt inte är kostnadseffektivt.

Riksrevisionens rekommendationer

Granskningen visar att myndigheternas arbete med informationssäkerhet har allvarliga brister. Riksrevisionen lämnar därför följande rekommendationer till regeringen.

- Myndigheterna har inte lyckats med att skapa ett informationssäkerhetsarbete som uppfyller kraven i MSB:s föreskrifter och därmed i den standard som ligger till grund för arbetet (ISO 27000). För att öka förutsättningarna att klara kraven rekommenderar Riksrevisionen regeringen att öka tydligheten i sin myndighetsstyrning, så att var och en av myndigheterna i statsförvaltningen uppnår god informationssäkerhet inom rimlig tid.
- Det finns ett behov av att komplettera MSB:s metodstöd vid riskanalyser för att bättre kunna ta till vara resultaten av de olika processerna och ställa samman dem till en övergripande enhet, så att allt nedlagt riskhanteringsarbete kommer till bästa nytta. Regeringen bör därför överväga att ge MSB i uppdrag att ta fram en modell eller ett metodstöd för hur myndigheterna på ett effektivt sätt kan samordna resultat och processer. Denna modell bör så långt det är möjligt stödja myndigheternas arbete med risker och med att ställa samman dem på ett hanterbart sätt. Det är också viktigt att regeringen genom sin myndighetsstyrning ser till att myndigheterna också tillämpar modellen.
- För att få ett effektivt skydd av informationstillgångarna i staten är det väsentligt att kunna göra avvägningar mellan kostnader och nytta. Det är inte möjligt i dag, eftersom kostnaderna för myndigheternas insatser för informationssäkerhet är okända. Det vore även angeläget att undersöka hur beslut om investeringar i informationssäkerhet sker i praktiken och vilka organisatoriska faktorer som påverkar synen på investeringar i informationssäkerhet. Regeringen bör därför låta utreda förutsättningarna för att visa samtliga kostnader förenade med informationssäkerhet för verksamheten i staten.
- Var och en av myndigheterna har att på egen hand pröva sig fram till hur de ska bedriva sitt informationssäkerhetsarbete. MSB:s vägledningar är bra, men det som fattas myndigheterna är ett operativt stöd. Riksrevisionen rekommenderar därför regeringen att överväga att låta utreda behovet av att inrätta en central funktion som skulle kunna få i uppdrag att lämna operativt stöd till myndigheterna.

1 Inledning

1.1 Bakgrund och motiv

I statsförvaltningen hanteras mycket information som är skyddsvärd. Det handlar om allt från information som hanteras inom ramen för myndighetsutövning mot enskilda till sådan information som avser rikets säkerhet. Informationssäkerhet innebär att se till att all skyddsvärd information är tillgänglig, riktig, konfidentiell och spårbar. Arbetet med att bygga och upprätthålla en god informationssäkerhet är en process som består av regler, rutiner och fysiska skyddsåtgärder. För att göra det behöver man införa ett ledningssystem som bland annat innebär att myndighetens information klassificeras utifrån tillgänglighet, riktighet och konfidentialitet samt att utifrån en riskanalys avgöra vilka åtgärder som behöver vidtas för att säkra informationen.[1] Informationssäkerhet är en fråga som berör samtlig personal i en myndighet. Det är alltså inte endast myndighetens ledning och säkerhetspersonalen som har ansvar för att bidra till att upprätthålla en god informationssäkerhet, utan alla som arbetar i en myndighet har detta ansvar.

Riksrevisionen granskade under åren 2005–2007 arbetet med informationssäkerhet vid elva myndigheter i statsförvaltningen.[2] Dessa myndigheter bedriver samhällsviktig verksamhet, hanterar mycket pengar, är starkt IT-beroende och hanterar skyddsvärd information. Informationssäkerhet var alltså en viktig förutsättning för verksamheten, något som i ännu högre utsträckning gäller i dag. Några exempel från 2015 är Arbetsförmedlingen som i genomsnitt hade cirka 664 000 arbetslösa inskrivna och transfereringar som uppgick till cirka 55 miljarder kronor, Försäkringskassan som betalade ut mer än 200 miljarder kronor och Migrationsverket som tog emot drygt 163 000 asylansökningar och betalade ut 21 miljarder kronor i bidrag.[3] Granskningarna av dessa myndigheter visade ett flertal brister när det gäller

---

1 I definitionen av ledningssystem ingår inte spårbarhet som en separat variabel, utan utgör i stället delmängder av tillgänglighet och konfidentialitet.

2 Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten (promemoria 2005, dnr 31-2004-1295), Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten (RiR 2005:27), Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten (RiR 2006:24), Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten (RiR 2006: 25), Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten (RiR 2006:26), Bolagsverkets informationssäkerhet (promemoria 2005, dnr 32-2005-0717), Granskning av Försäkringskassans interna styrning och kontroll av informationssäkerheten (revisionsrapport 2006, dnr 32-2005-0655), Post- och telestyrelsens informationssäkerhet (revisionsrapport 2006, dnr 32-2005-0738), Löpande granskning av Affärsverket Svenska Kraftnät 2005 (revisionsrapport 2006, dnr 32-2005-0714), Försvarsmaktens styrning av informationssäkerhetsarbetet (revisionsrapport 2006, dnr 32-2005-0551), Löpande granskning av Affärsverket Svenska Kraftnät 2006 (revisionsrapport 2007, dnr 32-2006-0700) samt Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen (RiR 2007:10).

3 Arbetsförmedlingens, Försäkringskassans respektive Migrationsverkets årsredovisningar för 2015.

myndigheternas arbete med informationssäkerhet. Regeringen hade inte följt upp om myndigheternas interna styrning och kontroll av informationssäkerhet var tillfredsställande, och regeringen hade inte heller gett myndigheterna tillräckliga förutsättningar för ett effektivt informationssäkerhetsarbete.

Under 2014 granskade Riksrevisionen ånyo informationssäkerhet. Denna gång undersöktes regeringen och dess stöd- och tillsynsmyndigheters styrning och stöd inom informationssäkerhetsområdet.[4] Granskningen visade att regeringen inte utövat en effektiv styrning. Den visade också att regeringens stöd- och tillsynsmyndigheter endast delvis hade vidtagit nödvändiga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas.

1.2 Syfte och avgränsningar

Syftet med denna granskning har varit dels att ånyo granska informationssäkerhetsarbetet vid de myndigheter som Riksrevisionen granskade 2005–2007, dels att bedöma om regeringen säkerställer att de granskade myndigheterna har en effektiv intern styrning och kontroll av sin informationssäkerhet.

Granskningen omfattar de myndigheter vars arbete med informationssäkerhet granskades av Riksrevisionen under åren 2005–2007, det vill säga Affärsverket svenska kraftnät, Arbetsförmedlingen, Bolagsverket, Försäkringskassan, Lantmäteriet, Migrationsverket, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk. Statens räddningsverk ingick i gruppen av myndigheter som granskades, men har upphört. Denna granskning är, liksom 2014 års granskning, inriktad mot den civila statsförvaltningen; därför ingår inte heller Försvarsmakten, som granskades vid den tiden. De utvalda myndigheterna bestämdes 2005 utifrån risk och väsentlighet, och utgör från storlekssynpunkt en betydelsefull del av statsförvaltningen.

Utöver dessa myndigheter omfattar granskningen även regeringen och dess kansli samt Ekonomistyrningsverket (ESV). ESV är berört eftersom myndigheten har ett särskilt utpekat ansvar för intern styrning och kontroll i statsförvaltningen.

Vi har granskat om myndigheterna utifrån dagens krav och förutsättningar bedriver ett informationssäkerhetsarbete på ett sådant sätt att de uppnår ett ändamålsenligt skydd av sina informationstillgångar. Det innebär även att vi har undersökt om det finns effektiva processer för att identifiera och hantera risker kopplade till informationssäkerhet.

[4] Riksrevisionens granskningsrapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23).

Det sätt på vilket regeringen styr och följer upp myndigheterna är avgörande för att den ska kunna förvissa sig om att statsförvaltningen är effektiv och kunna gå i god för att statens medel förvaltas på ett betryggande sätt.[5] Ett ytterligare moment i granskningen har därför varit att undersöka om regeringen har följt upp myndigheternas interna styrning och kontroll för arbetet med informationssäkerhet och om myndigheterna fått tillräckliga förutsättningar för att bedriva detta, så att de uppnår goda resultat.

För att informationssäkerheten ska vara effektiv, såväl för respektive myndighet, som för statsförvaltningen i stort krävs att det går att väga kostnader mot nytta. Därför har vi låtit en konsult undersöka kostnadsbilden.

1.3 Utgångspunkter

I denna granskning har Riksrevisionen utgått från följande bestämmelser
- 1 kap. 3 § budgetlagen (2011:203)
- 3 § och 4 § 4 myndighetsförordningen (2007:515)
- 2–5 §§ förordningen om intern styrning och kontroll (2007:603)
- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10)[6] med stöd av 30 a och 34 §§ förordningen (2006:942) om krisberedskap och höjd beredskap[7]
- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2015:3) med stöd av 9 och 34 §§ förordningen om krisberedskap och höjd beredskap[8]

Statlig verksamhet ska eftersträva hög effektivitet och god hushållning. Ledningen för en myndighet ska även säkerställa att det finns en intern styrning och kontroll som fungerar på ett betryggande sätt.[9] Av det följer, enligt Riksrevisionens bedömning, att myndigheterna i statsförvaltningen bör ha ett ändamålsenligt skydd för sin information. Informationssäkerheten utgör därmed en viktig del av den interna styrningen och kontrollen. Samtidigt utgör en betryggande intern styrning och kontroll en förutsättning för en god informationssäkerhet.

---

5 Departementspromemorian *Intern styrning och kontroll i staten* (Ds 2006:15), s. 17 f.

6 Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10) upphörde att gälla den 4 april 2016, då Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) började att gälla.

7 Förordningen (2006:942) om krisberedskap och höjd beredskap upphörde att gälla den 1 april 2016, då förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap började att gälla.

8 Ibidem.

9 1 kap. 3 § budgetlagen (2011:203) samt 3 § och 4 § 4 myndighetsförordningen (2007:515).

Med intern styrning och kontroll avses den process som syftar till att en myndighet med rimlig säkerhet bedriver sin verksamhet effektivt och rättsenligt samt att redovisningen är tillförlitlig och rättvisande. Denna process ska innehålla ett antal viktiga moment. För det första ska myndigheten göra en riskanalys för att identifiera omständigheter som utgör risk för att myndigheten inte lever upp till dessa krav. Med ledning av riskanalysen ska myndigheten vidta de åtgärder som är nödvändiga för att kraven ska fullgöras med rimlig säkerhet. Vidare ska den interna styrningen och kontrollen systematiskt och regelbundet följas upp och bedömas.[10]

Processen för intern styrning och kontroll bygger på den så kallade COSO-modellen.[11] För informationssäkerheten som sådan finns en standard för ledningssystem för informationssäkerhet (ISO 27000), som är införlivad i Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter om statliga myndigheters informationssäkerhet (MSBSF 2009:10). Även MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2015:3) är en utgångspunkt för denna granskning. Utifrån dessa normer har Riksrevisionen granskat områden som rör myndigheternas kontrollmiljö, organisering, riskanalyser, säkerhetsåtgärder, kontroll, uppföljning, information och utbildning.

Det ankommer på regeringen att försäkra sig om att myndigheternas ledningar lever upp till sitt förvaltningsansvar. Det är därför av betydelse för regeringen att myndigheternas interna styrning och kontroll fungerar väl. En förutsättning är att regeringen preciserar vad som avses med intern styrning och kontroll, och ställer tydliga krav på myndigheternas ledningar.[12] Om det finns brister kan regeringen behöva vidta åtgärder för att komma till rätta med dessa. Enligt Riksrevisionens mening innebär regeringens ansvar för intern styrning och kontroll att regeringen bör ställa tydliga krav på att myndigheterna bedriver ett arbete som leder till att ett ledningssystem är på plats och att det tillämpas i hela myndigheten. I detta ingår också att regeringen bör begära återrapportering om åtgärder är vidtagna och, om så inte skett, se till att det sker.

1.4 Genomförande

Vi har granskat Arbetsförmedlingen, Försäkringskassan och Migrationsverket särskilt ingående genom ett mätinstrument för status på informationssäkerhet.[13] Med

[10] 2–5 §§ förordningen (2007:603) om intern styrning och kontroll.

[11] Den amerikanska oberoende revisionsorganisationen *Committee of Sponsoring Organizations of the Treadway Commision* (COSO) har beskrivit intern styrning och kontroll i en särskild modell som kallas för COSO-modellen.

[12] Departementspromemorian *Intern styrning och kontroll i staten* (Ds 2006:15), s. 45.

[13] *Veriscan Rating*, tillhandahållet av Veriscan Security AB, som i huvudsak bygger på ISO-27000-standarden och är särskilt anpassat för Riksrevisionens granskning.

detta instrument har omkring 30 personer på respektive myndighet i olika befattningar och funktioner intervjuats med exakta, förutbestämda frågor anpassade till den roll och funktion personen har. Vi har på detta sätt intervjuat allt från styrelseledamöter och myndighetschefer via linjechefer till enskilda handläggare samt inte minst nyckelpersonal som arbetar med säkerhet.[14] Alla dokument på en myndighet som myndigheten har bedömt påverkar informationssäkerheten har också granskats med hjälp av mätinstrumentet.[15] Utöver detta har vi genomfört ett antal kompletterande och fördjupande intervjuer med nyckelpersoner inom säkerhetsarbetet på de granskade myndigheterna.

Mätningen på de tre myndigheterna är en prestandamätning som visar status på informationssäkerheten i förhållande till kraven i den standard (ISO 27001) för ledningssystem som myndigheterna, enligt MSB:s föreskrifter, ska tillämpa. Vi har mätt informationssäkerhetsarbetet när det gäller områdena organisation, system (IT) och riskhantering.[16] Varje område har brutits ned i kategorier, som i sin tur består av olika så kallade mätpunkter. Strukturen för detta framgår närmare av bilaga 2. Mätpunkterna belyser olika sidor av samma företeelse med utgångspunkt från perspektiven kunskap/medvetenhet, funktion samt reglering. Ett exempel: reglering kan mätas med utgångspunkt från både förekomst av en regel och kännedom om att den regeln finns.

Varje mätpunkt genererar ett resultat när alla intervjuer är genomförda på respektive myndighet. Resultatet kan variera från underkänt via godkänt till mer än godkänt. Resultaten från varje mätpunkt har sedan aggregerats för respektive kategori och sedan till de tre mätområdena organisation, system (IT) och riskhantering.

Övriga sex granskade myndigheter har besvarat en omfattande enkät som på ett mer övergripande sätt ringar in deras arbete med informationssäkerhet.[17] Efter det att enkätsvaren analyserats har vi besökt var myndighet på plats och med enkätsvaren som grund genomfört kompletterande, djupare intervjuer med personal som arbetar med informationssäkerhet. Vi har också tagit del av relevant dokumentation från dessa myndigheter.

För att belysa informationssäkerhetsarbetet ur aspekten intern styrning och kontroll har vi även granskat det stöd som ESV har lämnat. Vi har intervjuat berörda tjänstemän vid denna myndighet, och tagit del av relevant dokumentation. Vi har även

---

[14] När det gäller intervjuad personal som inte arbetar specifikt med säkerhet har urvalet skett på praktiskt möjligast sätt, vilket begränsar möjligheterna till generaliseringar.

[15] Sammanlagt har cirka 550 dokument från Arbetsförmedlingen, Försäkringskassan och Migrationsverket granskats.

[16] När det gäller riskhantering är utgångspunkten inte endast ISO-standarden, utan olika regelverk, och i den delen avviker mätningen från områdena organisation och system.

[17] Enkätformuläret redovisas i elektronisk bilaga 5, som finns tillgänglig på Riksrevisionens webbplats www.riksrevisionen.se.

intervjuat tjänstemän vid Finansdepartementet som ansvarar för frågor om intern styrning och kontroll. Dessutom har huvudmännen i Justitie-, Social- och Arbetsmarknadsdepartementen besvarat skriftliga frågor om intern styrning och kontroll av informationssäkerheten på Migrationsverket, Försäkringskassan och Arbetsförmedlingen.

I syfte att få uppgifter om kostnader för IT, IT-säkerhet och informationssäkerhet har vi låtit en konsult undersöka och jämföra dessa kostnader för statlig, kommunal och privat verksamhet.[18] Konsultrapporten redovisas i elektronisk bilaga 6.[19]

Som ett led i att säkerställa hållbarheten i våra iakttagelser och slutsatser har vi i slutet av granskningen genomfört ett externt seminarium med experter på informationssäkerhet. Dessa experter är Lars Nicander och Ingvar Hellquist från Försvarshögskolan/CATS[20], Fredrik Karlsson från Örebro universitet samt Jonas Hallberg från Totalförsvarets forskningsinstitut (FOI). Tidigare i granskningen, när preliminära resultat från de djupt granskade myndigheterna förelåg, genomfördes också ett seminarium med informationssäkerhetsansvariga från dessa myndigheter samt experter från Försvarets radioanstalt och MSB.

1.5 Rapportens disposition

Granskningsrapporten är disponerad på följande sätt:

I **kapitel 2** redogör vi för hur arbetet med informationssäkerhet ser ut på de granskade myndigheterna. Vi belyser resultaten av de djupgående granskningarna av informationssäkerhetsarbetet på Arbetsförmedlingen, Försäkringskassan och Migrationsverket samt redovisar iakttagelser från de andra granskade myndigheterna – Affärsverket svenska kraftnät, Bolagsverket, Lantmäteriet, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk.

Kapitel 3 söker fånga en bild av vilka kostnader som läggs ned på informationssäkerhet på myndigheter i statsförvaltningen i sin helhet.

Kapitel 4 handlar om vad regeringen och ESV gör när det gäller intern styrning och kontroll av informationssäkerhet.

[18] Radar Ecosystem Specialists: *IT- och informationssäkerhet – statliga myndigheter och verk, 2015–2016.*
[19] Den elektroniska bilagan finns tillgänglig på Riksrevisionens webbplats www.riksrevisionen.se.
[20] CATS står för Center for Asymmetric Threat Studies.

2 Arbetar myndigheterna systematiskt med informationssäkerhet?

Denna granskning visar att det ännu omkring tio år efter de granskningar Riksrevisionen då gjorde av informationssäkerhet finns allvarliga brister i myndigheternas arbete med informationssäkerhet. Granskningen visar även att det finns enskilda delar av arbetet som fungerar väl, vilket till stor del kan förklaras av vissa initiativ från enskilda individer eller delar av en verksamhet snarare än som ett resultat av ett systematiskt informationssäkerhetsarbete förankrat på ledningsnivå. Följaktligen finns det ett ansenligt behov av ännu fler insatser för att bygga upp och förvalta en informationssäkerhet som håller jämna steg med de ökande hoten som framkom genom Riksrevisionens förra granskning av informationssäkerhet.[21] I detta kapitel visar vi vad vi kommit fram till när det gäller dels de tre särskilt ingående granskade myndigheterna, dels de andra sex granskade myndigheterna. Vid redovisningen av resultaten för de djupare granskade myndigheterna anges deras status anonymiserat i noter, och i bilaga 3 finns en sammanställning därav.

Tre djupt granskade myndigheter
Arbetsförmedlingen, Försäkringskassan och Migrationsverket

Vi har genomfört fördjupade granskningar av hur arbetet med informationssäkerhet ser ut på Arbetsförmedlingen, Försäkringskassan och Migrationsverket.

Granskningen har skett i form av en prestandamätning som visar status på informationssäkerheten i förhållande till kraven i den standard (ISO 27001) som regleras i MSB:s föreskrifter. Granskningen omfattar de aspekter på informationssäkerhetsarbetet som handlar om organisation, IT-system samt riskhantering.[22]

Sex andra granskade myndigheter
Affärsverket svenska kraftnät, Bolagsverket, Lantmäteriet, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk

---

[21] Se Riksrevisionens granskningsrapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23).

[22] Redogörelsen för de fördjupade granskningarna i detta kapitel bygger på mätningar med programmet *Veriscan Rating* inklusive genomgång av relevant dokumentation samt på fristående intervjuer med säkerhetsansvariga på myndigheterna. Programmet har anpassats särskilt för denna granskning, där till exempel avdelningen Fysiskt skydd i huvudsak har utgått och Riskhantering tillkommit.

Vi har också granskat hur de sex andra tidigare granskade myndigheterna arbetar med sin informationssäkerhet. Granskningen bygger på en enkätundersökning, intervjuer samt dokumentstudier.[23]

2.1 Organisatoriska perspektiv på informationssäkerhetsarbetet vid de tre djupt granskade myndigheterna

Alla tre djupt granskade myndigheter är relativt likvärdiga när det gäller övergripande organisatoriska delar för informationssäkerhetsarbetet. Ingen av myndigheterna når dock upp till godkänt resultat.

2.1.1 Personal och informationssäkerhet

Generellt sett har de tre myndigheterna bra rutiner för vad som gäller vid anställning. Dessa rutiner inkluderar dock på två av myndigheterna generellt sett inte bakgrundskontroll eller säkerhetsprövning.[24] Alla myndigheter genomför utbildning för anställda där frågor om informationssäkerhet berörs, dock utan någon kontinuitet.

Alla tre myndigheter har genomfört tekniska åtgärder för att höja säkerheten på bärbara datorer, och den tekniska säkerheten för dessa är därför god. Två av myndigheterna har också tagit fram skriftliga regelverk för att hantera bärbara datorer. Dessa regelverk håller godkänd nivå.[25] Personalens kännedom om dessa regler är dock låg på alla tre myndigheter. Myndigheterna kontrollerar heller inte aktivt efterlevnaden av reglerna, utan endast när incidenter har rapporterats. Smarta telefoner och surfplattor, i den mån de används, har dock inte samma tekniska säkerhetsnivå och det saknas regler som styr vad som är tillåtet och inte. Dock krypteras e-post och kalenderfunktioner i smarttelefonerna. Alla tre myndigheterna sprider även information internt om säkerhetsrelaterade hot, varav en gör det rutinmässigt.[26]

2.1.2 Ledningens styrande dokumentation

Ingen av myndigheterna når upp till godkänd nivå när det gäller ledningens styrande dokumentation på en övergripande nivå. Riktlinjer för internetanvändning

[23] Redogörelsen för de andra granskningarna bygger i sin helhet på a) en enkätundersökning som besvarats av var och en av de sex myndigheterna, b) intervjuer med säkerhetsansvariga på samtliga dessa myndigheter samt c) genomgång av relevanta handlingar från dessa myndigheter såsom styrelseprotokoll, protokoll eller minnesanteckningar från ledningsgruppsmöten, riskanalyser, externa och interna granskningar av informationssäkerheten, m.m.

[24] Myndighet A har riktlinjer som rör bakgrundskontroll.

[25] Myndighet A och C uppnår godkänt medan myndighet B inte uppnår godkänd nivå.

[26] Myndighet B bedöms ha en rutinmässig spridning.

saknas på en av myndigheterna[27] och är bristfälliga på de övriga två. Alla tre myndigheter har en informationssäkerhetspolicy där det tydligt framgår att det är en viljeyttring från ledningen och gäller för hela myndigheten. Det är dock endast en myndighet[28] som indikerar att arbetet med informationssäkerhet är riskdrivet och ska förverkligas genom insatser som exempelvis riskanalys, utbildning, incidenthantering och kontinuitetshantering. Personalens kännedom om informationssäkerhetspolicyn är låg på alla tre myndigheterna. Generellt sett kan personalen inte redogöra för vad policyn har för syfte och funktion och var den finns att tillgå. Personalen har också låg medvetenhet om informationsklassificering och hur den tillämpas i praktiken.[29]

2.1.3 Incidenthantering

Två myndigheter har en otillräcklig organisation för att hantera incidenter.[30] Bristerna består främst i att insamling och utvärdering inte sker på ett strukturerat sätt. Det saknas även en gradering av incidenterna efter hur allvarliga de är samt en process med tydliga roller och ansvarsfördelning när det handlar om vem som ska rapportera till ledningen när det är nödvändigt. Ingen av myndigheterna har heller en tydlig process, som omfattar hela verksamheten, för att systematiskt identifiera orsakerna till incidenterna. Personalen vid alla tre myndigheterna har också låg kännedom om vilka regler som finns för att hantera incidenter och hur de ska gå till väga om en incident inträffar.

2.1.4 Hanteringen av informationstillgångar

Ingen av de tre myndigheterna når upp till godkänd nivå när det gäller att hantera sina informationstillgångar. Alla tre myndigheter har förvisso en metod för att klassificera informationen, som täcker in tillgänglighet, riktighet och konfidentialitet. Två av myndigheterna har enligt riktlinjen som krav att klassificeringsmetoden ska gälla för all information, men det kravet efterlevs inte operativt.[31] Den tredje myndigheten tillämpar endast sin metod för digital information. Ingen av myndigheterna tillämpar informationsägarskap fullt ut på så sätt att det är definierat vad ansvaret för det innebär, det vill säga att det är dokumenterat, formellt godkänt och

---

27 Myndighet C. Myndigheten har vid faktagranskningen framfört att man har vissa riktlinjer på intranätet, men att dessa är bristfälliga.

28 Myndighet C

29 Det vill säga att man kan beskriva innebörden av informationsklasser, även om man inte använder begreppet uttryckligen.

30 Myndighet B och C.

31 Myndighet A och C.

definierat i en roll i form av informationsägare. Det är sällan som kärnverksamheten ställer krav på säkerhet i de system som används. Det är snarare säkerhets- och IT-funktioner som ställer krav på säkerhet.

Ingen av myndigheterna når upp till godkänd nivå i fråga om att säkra nyckelkompetens. En av myndigheterna säger sig ha identifierat nyckelpersoner, men har inte vidtagit några mer omfattande åtgärder på grund av det. [32] De två övriga myndigheterna uppger att problemet är känt, men har inte i någon större omfattning identifierat nyckelpersoner.

2.1.5 Analys och kontroll

Ingen av myndigheterna når upp till godkänd nivå när det gäller analys och kontroll av informationssäkerhet på övergripande nivå.

Samtliga myndigheter har en modell som stöder verksamhet som bedrivs i projekt. Modellen är baserad på riskanalys och inbegriper även informationssäkerhetsaspekter. Två myndigheter har en modell som ska säkerställa att informationssäkerhetsaspekter blir bedömda och tillvaratagna.[33] Av dessa två är det endast en myndighet som tydligt säkerställer att bedömningen av informationssäkerhetsaspekterna sker tidigt i projektet.[34] En av myndigheterna har delvis genomfört en kontinuitetsplanering för kritiska funktioner. Samma myndighet har till viss del även testat dessa planer, dock inte regelbundet.[35] De två övriga myndigheterna har inte en kontinuitetsplanering som når upp till godkänd nivå.

Samtliga tre myndigheter genomför sporadiska riskbedömningar med koppling till konfidentialitet, riktighet och tillgänglighet. Ingen av myndigheterna utför dock regelbundna och övergripande analyser som fokuserar på informationssäkerhet. De analyser som ändå berör informationssäkerhet gäller endast enskilda system.

2.1.6 Informationssäkerhetsledning

Av intervjuerna med företrädare för organisationen framgår att i samtliga myndigheter anses ledningen ha det yttersta ansvaret för informationssäkerheten. Det finns också ett uttalat särskilt ansvar i form av att leda och samordna arbetet. Det ansvaret är dock delegerat långt ned i organisationen, utan tillräckliga befogenheter och resurser.

För att åstadkomma ett systematiskt informationsarbete ska myndigheterna enligt MSB:s föreskrifter utforma ett ledningssystem för informationssäkerhet. En viktig

[32] Myndighet C.
[33] Myndighet A och B.
[34] Myndighet B.
[35] Myndighet A.

del av ledningssystemet är den årligen återkommande så kallade *ledningens genomgång*. Syftet med denna genomgång är att den högsta ledningen, som har det yttersta ansvaret, ska kunna säkerställa systemets fortsatta lämplighet, tillräcklighet och verkan. Genomgången är en förutsättning för att kunna besluta om förbättringar och att möjliggöra att ledningssystemet följer den så kallade PDCA-cykeln[36] eller annan likvärdig metodik. Granskningen visar dock att ingen av myndigheterna har haft någon sådan genomgång de senaste två åren.

En annan viktig del av ett ledningssystem är regelbunden utvärdering. Ingen av myndigheterna utvärderar dock sitt ledningssystem till väsentliga delar eller med den periodicitet som krävs. Därför saknar myndigheterna tillräckligt underlag för att kunna bedöma om ledningssystemet fungerar eller inte.

2.1.7 Skalskydd

Samtliga tre myndigheter har ett skalskydd som bedöms som tillräckligt. Passerkort eller bricka används för inpassering dygnet runt och utanför kontorstid krävs även kod. För känsligare utrymmen används säkerhetszoner, som alltid kräver såväl kod som kort eller bricka. Man har även en loggfunktion kopplad till passersystemet. Alla tre myndigheter har dessutom regler för att reducera risker när man tar emot besökare. Reglerna är uttalade och inkluderar ansvaret för den besökande samt registrering och avregistrering. Två av myndigheterna kontrollerar även efterlevnaden av dessa regler.[37]

2.2 Organisatoriska perspektiv på informationssäkerhetsarbetet vid de sex andra granskade myndigheterna

Informationssäkerhetsarbetet är organiserat på olika sätt vid de sex andra granskade myndigheterna. Vid en av myndigheterna är informationssäkerhetsansvarig en chef direkt underställd generaldirektören och därmed också medlem i myndighetens ledningsgrupp. Vid en annan myndighet finns den ansvariga på lägsta möjliga organisatoriska nivå. På de övriga myndigheterna befinner sig ansvariga på olika nivåer däremellan. Eftersom informationssäkerhet även inbegriper IT-säkerhet finns det också personal från IT-funktioner som delvis arbetar informationssäkerhetsrelaterat. Fyra av myndigheterna har därtill kontaktpersoner på avdelningar inom kärnverksamheten som har informationssäkerhet som tillikauppdrag vid sidan av sina ordinarie arbetsuppgifter i linjen. Vid de andra två myndigheterna finns, i stället för kontaktpersoner, forum för säkerhets- respektive IT-frågor där informationssäkerhet kan avhandlas. Vid en av myndigheterna är den chef som är ansvarig för

[36] PDCA står för Plan, Do, Check, Act, det vill säga Planera, Utföra, Studera, Agera, och är en metod inom kvalitetstekniken för systematiskt förbättringsarbete.

[37] Myndighet A och B.

informationssäkerheten adjungerad till detta forum. Denna person har dock aldrig blivit kallad till något möte.

2.2.1 Ledningssystem för informationssäkerhet

Alla de granskade myndigheterna har en policy för informationssäkerhet. Efterlevnaden varierar dock mellan myndigheterna.

Det finns flera förklaringar till att efterlevnaden varierar. En förklaring som myndigheterna lämnat är att ledningssystemet inte har uppdaterats och därför blivit föråldrat, en annan är att det är svårt att få människor att följa regler rent allmänt. En av myndigheterna har angett att bristande kunskap och svag ekonomi gjort att säkerhetsarbetet fått stå tillbaka. En annan myndighet har sagt att de medvetet gått långsamt fram med att genomföra informationsklassningen för att inte störa kärnverksamheten mer än nödvändigt och för att få bättre kvalitet i genomförandet. Ytterligare en myndighet uppger att den agerat pragmatiskt och gjort kontinuerliga förbättringar efter rådande lägesbild, i stället för att vänta på att ett perfekt system ska vara på plats. En annan sak som kan förklara bristerna i efterlevnad, och även bristerna i säkerheten, är att endast två av myndigheterna säger att de systematiskt och regelbundet följer upp att beslutade åtgärder verkligen genomförs.

Endast en myndighet anger att den fullt ut tillämpar de standarder som ska ligga till grund för ledningssystemet. För de övriga myndigheterna varierar det hur mycket de tillämpar dessa standarder.

2.2.2 Ansvar, roller och kompetens

När Riksrevisionen under perioden 2005–2007 granskade samma myndigheter visade det sig att det ofta var problem med nomenklaturen när det gäller ansvar och roller i säkerhetsarbetet. Detta problem kvarstår inte i dag, vilket gör att tydligheten i säkerhetsarbetet har ökat. Däremot finns det kvarstående problem med att säkerställa att nyckelpersoner får den utbildning de behöver, så att de besitter rätt kompetens. Några myndigheter anser att det är svårt att säkerställa detta, några andra har svarat att de inte har säkerställt det.

När det kommer till övrig personal varierar omfattningen på utbildningsinsatserna. Tyngdpunkten ligger för det mesta på nyanställda, men behovet av återkommande utbildning för redan anställda är uppmärksammat.

2.2.3 Incidentrapportering

Det är viktigt att kunna ha tillgång till en samlad lägesbild över hot, risker, händelser och vidtagna skyddsåtgärder för att kunna skapa nödvändig säkerhetsförmåga. En av flera nödvändiga komponenter i detta är att det finns en väl fungerande och heltäckande incidentrapportering.

Två myndigheter uppger att de har en samlad lägesbild som omfattar risker, skyddsåtgärder och händelser. Dock har en av dem uppgett att de inte har en systematisk incidentrapportering. Det talar sannolikt för att denna myndighets lägesbild är behäftad med brister.

2.2.4 Planering

Planeringen för informationssäkerheten och för att kunna fortsätta verksamheten om det inträffar en händelse uppvisar brister.

Två av de granskade myndigheterna har en övergripande plan för sin informationssäkerhet. Ingendera planen innehåller dock uppgifter om vilka skyddsåtgärder som är beslutade, inte heller vilka personer som i så fall skulle ansvara för att genomföra åtgärderna.

Av enkätundersökningen framgår att det ser bättre ut när det gäller kontinuitetsplanering. Fyra av myndigheterna uppger att de har en kontinuitetsplan eller motsvarande. Två av dessa planer täcker in omfattande delar av verksamheten, varav en dock har brister i fråga om IT. Två av dessa myndigheter har planer som täcker in endast IT. Myndigheterna har svarat att planerna övas i viss utsträckning.

Vid två av de granskade myndigheterna finns en samlad åtgärdsplan som gör det möjligt för myndigheternas ledning att bli informerad om vilka skyddsåtgärder som är genomförda. En myndighet uppger att den saknar kontroll över vilka åtgärder som faktiskt blir genomförda.

2.2.5 Ledningens stöd[38]

Överlag uppfattar de som arbetar med informationssäkerhet att myndigheternas ledning stöder arbetet med informationssäkerhet. Sett till vad som i övrigt visat sig under granskningen finns det starka skäl som talar för att stödet ändå inte är till fyllest. Vi bedömer att det finns utsagor som också tyder på att stödet från ledningen varierar mellan myndigheterna. Till exempel är det en myndighet där ledningen har liten förståelse och lågt engagemang, och där behov endast blir tillgodosedda om så oundgängligen måste ske.[39]

Vi har också undersökt hur ofta under 2015 som styrelse och ledning har behandlat frågor om informationssäkerhet eller frågor som kan ha beröringspunkter med detta område. Fem av de granskade myndigheterna har en styrelse, en är enrådigt styrd.

Det är få gånger som informationssäkerhet har behandlats i myndigheternas styrelser. Som mest har det skett två gånger i två styrelser, en gång i två styrelser och

---

38 Detta avsnitt bygger enbart på intervjuer och dokumentstudier på de sex granskade myndigheterna.

39 Intervjuer på de sex myndigheterna.

ingen gång i en styrelse. Ärendena är för det mesta av strategisk karaktär, och handlar till exempel om att godkänna eller presentera upplägg för riskanalys enligt förordningen om intern styrning och kontroll, redovisa riskanalys enligt förordningen om krisberedskap och höjd beredskap eller att anmäla att Säkerhetspolisen har påpekat att det bör ske en säkerhetsanalys enligt säkerhetsskyddsförordningen.[40]

I ledningsgrupperna har frågor om informationssäkerhet behandlats oftare: i tre ledningsgrupper har det skett mellan sex och sju gånger, i två grupper två gånger och i en är det okänt eftersom minnesanteckningar från ledningsgruppens möten inte förs vid den myndigheten. Ärendena i ledningsgrupperna kan ligga både på strategisk nivå och operativ nivå. Exempel på ämnen är kontinuitetsplanering, redovisning av störningar, incidenthantering, riktlinjer för elektronisk utrustning, integrering av ledningssystem för informationssäkerhet med övrigt ledningssystem, olika lägesrapporter, etc. Ämnena varierar i fråga om hur mycket de berör informationssäkerhet. Värt att nämna är att i ledningsgruppen vid en av myndigheterna finns ett ärende som i sin helhet berör just hur det går med informationssäkerhetsarbetet.[41]

2.3 Systemperspektiv (IT) vid de tre djupt granskade myndigheterna

Systemperspektivet har bäring på IT-området och är en viktig beståndsdel i informationssäkerheten. Det handlar om hantering av behörigheter och vilka kontrollsystem som finns. Spårbarhet utgör också en del av systemperspektivet.

2.3.1 Behörigheter och kontrollsystem

Alla tre myndigheter dokumenterar behörighet till olika typer av information. Samtidigt dokumenteras dock inte alla förändringar i behörigheter, vilket gör att det sannolikt förekommer odokumenterade behörigheter. Alla tre myndigheter administrerar sina användaridentiteter med tydliga steg (ansökan, godkännande och genomförande) när en behörighet ska tilldelas eller ändras. För två av myndigheterna sker detta främst för vanliga användare, under det att systemadministrativa behörigheter hanteras mer informellt. Vid den tredje myndigheten är det ingen skillnad i hanteringen av behörigheter mellan vanliga användare och systemadministratörer.[42]

Alla tre myndigheter har ett behörighets- och kontrollsystem som reglerar kontroll av tillgång till information och vilken roll den person har i organisationen som ska

[40] Genomgång av protokoll från styrelsemöten under 2015 vid fem av de granskade myndigheterna.
[41] Genomgång av minnesanteckningar från ledningsgruppsmöten vid fem av myndigheterna.
[42] Myndighet A.

ha tillgång till viss information. En eller flera roller kan tilldelas en individ, och används för att avskilja tillträde till informationen. Vid två av myndigheterna saknas dock en formell koppling till individens arbetsuppgifter i systemet. Den tredje myndigheten har däremot ett behovsprövat system för att ge tillträde till information där rollen är anpassad till individens identitet i systemet och arbetsuppgifter.[43]

2.3.2 Ledningens styrande dokumentation

En av de tre myndigheterna har en lösenordspolicy som når upp till godkänt.[44] För de andra två myndigheterna är kraven på längd, komplexitet och giltighetstid inte uppfyllda i policyn.[45] Personalens kännedom om säker lösenordshantering är låg i alla tre myndigheterna.[46]

En av myndigheterna har en rutin för att kontrollera åtkomsten till sina verksamhetssystem, som dock endast används sporadiskt.[47] Två av myndigheterna har en rutin som alltid används, och det går att få en förteckning av alla loggningar som gjorts. Av dessa två är det dock endast en som har en dokumenterad rutin som innehåller en tydlig beskrivning av hur verksamheten ska rapportera förändringar och där förteckningen revideras minst årligen.[48]

Alla tre myndigheter har regler för hur säker utveckling ska ske. Vid en av myndigheterna har de funktioner som ansvarar för styrning och uppföljning av utvecklingsprojekt även ett ansvar för att följa upp efterlevnaden av dessa regler.[49]

Alla tre myndigheter har dokumenterade regler för fjärranslutning av utrustning som personalen har blivit delgiven. Alla tre myndigheter använder teknisk implementation i form av VPN[50] och tvåfaktorsautentisering[51], vilket innebär en väsentligt minskad risk vid fjärranslutning.

---

43 Myndighet C.

44 Myndighet A.

45 Riksrevisionen har dock inte granskat kvaliteten på lösenordshanteringen per se. En av myndigheterna har vid faktagranskningen uppgett att den endast undantagsvis använder lösenord; i stället används inloggningskort med certifikat och PIN-kod.

46 Samtidigt använder samtliga tre myndigheter tekniska lösningar i form av tvåfaktorautentisering och VPN-teknik för att användaren ska kunna nyttja datorutrustningen varför bristerna i lösenordspolicyn inte torde innebära någon större risk för verksamheten överlag.

47 Myndighet B.

48 Myndighet A.

49 Myndighet B.

50 VPN står för Virtuellt Privat Nätverk och är en teknik som används för att skapa säkra förbindelser mellan två punkter i ett icke-säkert datanätverk.

51 Tvåfaktorsautentisering är en extra säkerhetsnivå som ser till att det endast är en behörig användare som kan komma åt sparade uppgifter.

2.3.3 Spårbarhet och drift

Ingen av myndigheterna når upp till godkänd nivå när det gäller reglering av spårbarhet i revisionsloggar. En myndighet saknar skriftliga bestämmelser för säkerhetsloggning.[52] De två andra myndigheterna har regler för spårbarhet som omfattar de viktigaste begreppen i form av tid, användaridentitet och otillåten användning. Det saknas dock bestämmelser om att lösenord inte får loggas.[53] Alla tre myndigheter tillämpar personliga identiteter för samtliga användare vid inloggning i IT-systemen. Gruppidentiteter förekommer i begränsad omfattning och sker behovsprövat med god kontroll. Systemadministrativa konton samutnyttjas dock i viss grad.

Vad gäller avveckling av datamedier saknar en av myndigheterna regler för hur dessa ska avvecklas.[54] De två andra myndigheterna har dokumenterade regler som beskriver hur datamedier ska avvecklas, men endast en av dem[55] har regler som är sanktionerade hos ledningen.

Säkerhetsansvaret för myndighetens WLAN[56] finns muntligt uttalat på två av myndigheterna. På den tredje myndigheten finns detta ansvar dokumenterat i form av arbetsbeskrivningar, befattningsbeskrivningar eller motsvarande.[57]

Två myndigheter har rutiner för säkerhetskopiering, vilket innebär att de uppnår högsta möjliga nivå i mätningen. Säkerhetskopieringen genomförs automatiskt på de mest väsentliga systemen. Backupschema, omfattning och frekvens är tydliga och lagringen av backuper sker på annan fysisk plats än för originaldata. Informationen om vad som ska säkerhetskopieras och hur det ska ske finns lättillgängligt på annan media än i själva verktyget för säkerhetskopiering och två personer eller fler kan hantera säkerhetsfunktionen och återläsa data. Den tredje myndigheten når inte upp till godkänt, eftersom backuperna förvaras på samma fysiska plats som originaldata.[58]

2.4 Systemperspektiv vid de sex andra granskade myndigheterna

I den enkätundersökning som genomfördes på de sex myndigheterna fanns två frågor om IT-säkerhet. Frågor om IT-säkerhet ställdes också vid intervjuerna på de sex

52 Myndighet C.

53 En av myndigheterna har vid faktagranskningen uppgett att alla lösenord som används är krypterade, och att tangenttryckningar inte loggas.

54 Myndighet C.

55 Myndighet A.

56 WLAN står för Wireless Local Area Network och är ett samlingsnamn för olika typer av trådlösa lokala datornätverk.

57 Myndighet C.

58 Myndighet B.

myndigheterna. Svaren indikerar att myndigheterna har ett relativt sett något bättre grepp om just IT-säkerhet än om informationssäkerhet i stort.

Fem av myndigheterna uppger att de har dokumenterade regler för såväl hantering av fjärranslutningar till myndigheternas IT-miljö som regler för behörigheter. En av myndigheterna uppger att detta i stort sett saknas.

2.5 Riskhantering vid de tre djupt granskade myndigheterna

En central del i Riksrevisionens granskning har varit att undersöka hur myndigheterna organiserar och utför sin riskhantering. I en allt mer komplex värld där resurserna är begränsade blir riskhantering ett viktigt verktyg för att fördela resurser till de områden där de gör mest nytta. I denna granskning har vi framför allt identifierat tre områden där riskhantering har koppling till informationssäkerhet. Det är MSB:s föreskrifter om statliga myndigheters informationssäkerhet som innehåller bestämmelser om ledningssystem (LIS), MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser samt myndighetsförordningen och förordningen om intern styrning och kontroll som också dessa omfattar krav på riskanalys.[59]

Även om varje område innebär separata krav på riskhantering är den bärande tanken bakom bestämmelserna om intern styrning och kontroll att denna ska integreras med myndighetens ordinarie verksamhetsstyrning och uppföljning. Regeringen har uttryckt att arbetet med riskhantering ur ett krisberedskapsperspektiv ska samordnas med myndighetens övriga riskhantering för att uppnå högre effektivitet.[60] Även om processen för intern styrning och kontroll formellt sett inte är överordnad de två övriga riskhanteringsprocesserna, anser vi att det är rimligt att se de två andra riskhanteringsprocesserna som komplementära med den övergripande interna styrningen och kontrollen. Vi har därför önskat belysa hur arbetet med att hantera risker inom de tre perspektiven bedrivs samt hur resultatet från de olika områdena slutligen samordnas och aggregeras. Därför belyser granskningen riskhantering enligt alla dessa tre områden.

---

[59] Det finns även andra krav på att myndigheter ska analysera och hantera risker, bland annat ur arbetsmiljöperspektiv eller försäkringsperspektiv. Dessa områden har dock inte någon direkt bäring på just informationssäkerhet. De krav på riskhantering som säkerhetsskyddslagen och säkerhetsskyddsförordningen ställer har dock en direkt bäring på informationssäkerhet. Då detta är ett område som omgärdas av stark sekretess, vilket försvårar hanteringen i en öppen rapport, har det exkluderats från granskningen.

[60] Prop. 2010/11:1 UO6, s. 73.

2.5.1 Modeller för intern styrning och kontroll

Alla tre myndigheter har en modell för att arbeta med sin interna styrning och kontroll. De har även i sina styrdokument integrerat processerna för myndighetens riskhantering med verksamhetens processer för planering och uppföljning. Myndigheterna har även tagit fram någon form av handläggarstöd för riskhantering som styr hur riskhanteringen generellt sett ska bedrivas. En av myndigheterna har i sina riktlinjer för intern styrning och kontroll organiserat arbetet i vad man kallar försvarslinjer. Den första försvarslinjen i myndigheten utgörs av de primära riskägarna, vilket följer av hur myndigheten är organiserad. Den första försvarslinjen utgörs av avdelningar och staber och ytterst av respektive avdelnings- eller stabschef. Ansvaret innebär att hantera risker och upprätthålla en systematisk, transparent och effektiv intern styrning och kontroll på samtliga nivåer inom sin organisatoriska del. Den andra försvarslinjen är funktionellt orienterad mot dem som ansvarar för väsentliga moment för intern styrning och kontroll i vid mening. Funktionerna har inslag av både stödjande och övervakande roller, till exempel ekonomistab och säkerhetsstab. Den tredje försvarslinjen är internrevisionen.

De två andra myndigheterna har inte lika utförliga modeller för riskhantering; där är ansvaret för riskhantering i stort reglerat utifrån rollen som chef. De processer som finns för att specifikt hantera risker när det gäller informationssäkerhet ser dock i huvudsak likadana ut i alla tre myndigheter. Varje avdelnings-, stabs- eller enhetschef har ansvar för att analysera risker och vidta nödvändiga åtgärder. Risker som beror på nyutveckling eller förändring av IT-system hanteras dock genom analyser för det specifika systemet.

2.5.2 Tillvägagångssätt

Risk- och sårbarhetsanalyser ur ett krisberedskapsperspektiv ska i två av myndigheterna utföras av kärnverksamheten med stöd av säkerhetsstaben. Säkerhetsstaben ansvarar för att sammanställa och analysera materialet och vid behov föra in risker i myndighetens övergripande riskanalys inom intern styrning och kontroll. I den tredje myndigheten har säkerhetsstaben haft i uppdrag att ta fram en risk- och sårbarhetsanalys, dock utan att det är uttalat att kärnverksamheten ska bidra.[61]

Alla tre myndigheter har någon form av riktlinjer och metodik för riskanalys generellt. Två av myndigheterna graderar risk utifrån sannolikhet och konsekvens i en fyrgradig skala medan den tredje ganska nyligen har slutat med detta när det gäller hanteringen enligt förordningen om intern styrning och kontroll.[62] Skälet är att det blev för stort fokus på graderingen snarare än att hitta och åtgärda risker. I alla tre

[61] Myndighet C.
[62] Myndighet B.

myndigheter finns riktlinjer för eskalering, det vill säga för när frågan ska lyftas högre upp i organisationen.

Alla tre myndigheter har verksamhetscontrollers på olika nivåer i organisationen, som stöder kärnverksamheten vid riskanalys. Det finns också etablerade controllernätverk där frågor om riskanalys kan diskuteras. Resurserna för styrning och uppföljning av myndighetens riskhantering på den myndighetsövergripande nivån består av 2–3 personer på respektive myndighet.

2.5.3 Riskidentifiering

Riskidentifieringsprocessen ingår i den löpande uppföljningen och är en integrerad del av verksamhetsplaneringen. Trots att myndigheterna lägger ned mycket tid på arbetet med riskanalys går det inte, utifrån de uppgifter om genomförda riskanalyser som Riksrevisionen fått del av, att bedöma kvaliteten på riskhanteringen. Av granskningen framgår att det finns en övergripande riskanalys med risker, åtgärder, värderingar och riskägare. Det framgår också att riskhanteringen har följts upp och att cheferna har fått bedöma om hanteringen har varit betryggande. Det framgår dock även att det inte finns någon dokumentation av på vilket sätt riskanalysen har genomförts; tonvikten ligger snarare på att någonting har blivit gjort än hur det gått till och med vilken kvalitet.

En av myndigheterna har inte gjort någon risk- och sårbarhetsanalys ur ett krisberedskapsperspektiv.[63] För en av de två myndigheter som har genomfört en sådan risk- och sårbarhetsanalys är det svårt att bilda sig en uppfattning om krisberedskapsförmåga när det gäller informationssäkerheten.[64] Det går heller inte att se någon tydlig koppling mellan risk- och sårbarhetsanalysen, som görs utifrån ett krisberedskapsperspektiv, och myndighetens övergripande riskanalys. Den tredje myndigheten har tagit fram en risk- och sårbarhetsanalys i vilken man till viss del kan se att risker har förts över från den analysen till myndighetens övergripande riskanalys.[65] Av underlagsmaterialet till risk- och sårbarhetsanalyserna går det dock inte att göra någon kvalitativ bedömning av själva analysen då det saknas beskrivning av metod, ingångsvärden, m.m.

2.5.4 Vem har egentligen ansvaret?

I de intervjuer som Riksrevisionen gjort på myndigheterna framkommer att medarbetare och chefer inom kärnverksamheten i huvudsak anser att ansvaret för informationssäkerhet ligger på säkerhets- eller IT-funktionerna. Personalen har generellt sett svårt att se sitt eget ansvar för informationssäkerheten, vilket i förläng-

63 Myndighet C.
64 Myndighet B.
65 Myndighet A.

ningen kan innebära att informationssäkerhetsrisker inte framkommer i de riskanalyser som genomförs inom kärnverksamheten. Majoriteten av de risker som identifieras och återges i myndigheternas övergripande riskanalys är risker kopplade till strategisk och operativ styrning. Risker med bäring på informationssäkerhet saknas i stor utsträckning i två av myndigheternas riskanalyser[66], och förekommer endast till viss del i den tredje myndighetens.

Myndighetsledningarnas engagemang och ställningstagande i fråga om riskhantering och det praktiska riskidentifieringsarbetet är inte tillräckligt tydligt kommunicerat. Det är inte myndighetsledningen som för ut budskapet om riskhantering i organisationen, utan det är delegerat till respektive chefsnivå. I en av myndigheterna[67] har internrevisionen nyligen granskat riskhanteringen och där framkommer att styr- och stöddokument inte alltid når ut till alla chefer, vilket gör att arbetet med att identifiera risker i flera fall tenderar att ske ad hoc i stället för systematiskt. Revisionen kunde också visa att processen för att identifiera risker inte alltid bidrar till ett mervärde, varför dokumentationen blir en pappersprodukt som inte hålls levande. Vidare framkom att vissa avdelningar och staber med ansvar för specifika riskanalyser inte på ett samlat och systematiskt sätt har kunnat redogöra för hur de bedriver arbetet. Arbetet med specifika riskanalyser är således inte tillräckligt transparent, och det saknas en koppling till de organisatoriska riskanalyserna.

2.5.5 Strukturen varierar

Myndigheterna har i huvudsak en struktur för riskanalys och riskhantering på plats när det gäller intern styrning och kontroll. Det finns i varierande utsträckning stöddokument, metodbeskrivningar, rutiner för eskalering, m.m. Samtliga tre myndigheter genomför även systemsäkerhetsanalyser, och två av myndigheterna genomför risk- och sårbarhetsanalyser ur ett krisberedskapsperspektiv. I flera av intervjuerna framkommer dock synpunkter på att myndigheterna har skapat en struktur eller process som på papperet uppfyller kraven på intern styrning och kontroll, men att man inte avsätter tillräckligt med resurser för att skapa en kvalitativ riskhantering de facto. En möjlig förklaring är att förordningen om intern styrning och kontroll ställer krav på processen, snarare än det resultat som processen ska uppnå.

Alla tre myndigheter genomför riskanalyser med olika syften i skilda delar av organisationen, ofta med överlappningar. Ingen av myndigheterna genomför dock någon myndighetsövergripande riskanalys med fokus på informationssäkerhet och som kopplar samman systemsäkerhetsanalyser och krisberedskapsanalyser med analyser i kärnverksamheten. Ingen av myndigheterna har heller genomfört någon övergripande planering med riskanalys som grund för prioriteringar i arbetet med informationssäkerhet.

---

66 Myndighet B och C.

67 Myndighet A.

2.6 Riskhantering vid de sex andra granskade myndigheterna

Granskningen visar att riskanalyser vid de sex andra granskade myndigheterna tas fram på varierande sätt, och att det finns brister såväl i genomförandet som i den vidare hanteringen av riskerna.

Ett viktigt underlag för riskanalysen är att klassificera informationstillgångarna efter konfidentialitet, tillgänglighet och riktighet. Alla sex myndigheter uppger att de har en metod för att klassificera sina informationstillgångar. Två av myndigheterna har också kommit så långt att de kunnat upprätta en samlad förteckning av samtliga tillgångar. Dock framgår inte om några åtgärder har vidtagits till följd av resultatet av klassificeringen. För en av myndigheterna framgår inte heller vilka beroendeförhållanden som finns mellan tillgångarna då man ännu inte hunnit med att göra det.

Fyra myndigheter har svarat att de genomför en systematisk riskanalys inom ramen för informationssäkerhetsarbetet. En annan av myndigheterna analyserar dessa risker ad hoc vid större förändringar i system till exempel. Ytterligare en annan myndighet har tagit fram en process för att göra en systematisk riskanalys. De analyser vi tagit del av skiljer sig såväl i framtagning och utformning som efter vilket regelverk de är framtagna från.[68] Detta utgör dock inte något fel i sig, men gör en samlad bedömning komplicerad.

Tre av myndigheterna gör en årligen återkommande riskanalys. För fem av myndigheterna omfattar analysen hela verksamheten. För tre av myndigheterna omfattar analysen alla fyra parametrarna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Två av myndigheterna har analyser som inte omfattar någon av dessa parametrar.

På fråga om myndighetsledningen efter riskanalys tagit ställning till vilka risker de är beredda att ta och vilka som ska minskas, undvikas eller kvarstå uppger två myndigheter att ledningen har gjort det. Vid övriga myndigheter har så inte skett.

2.7 Myndigheterna måste göra allt

Denna granskning har visat att det är en tung uppgift för myndigheter att bedriva ett framgångsrikt informationssäkerhetsarbete. MSB bistår med bra vägledning för hur en myndighet ska arbeta med informationssäkerhet. Flera av de granskade myndigheterna uppger dock att det är långt ifrån tillräckligt och att de faktiskt lider

---

[68] MSB:s föreskrifter om ledningssystem för informationssäkerhet (MSBFS 2009:10), förordningen (2007:603) om intern styrning och kontroll, förordningen (2006:942) om krisberedskap och höjd beredskap, förordningen (1995:1300) om statliga myndigheters riskhantering samt säkerhetsskyddsförordningen (1996:633). Den senare gäller i fråga om säkerhetsanalys.

brist på operativt bistånd, något som MSB inte erbjuder i dag. Flera myndigheter har uppgett att man får, som det heter, uppfinna hjulet på egen hand i alltför stor utsträckning.[69]

[69] Intervjuer på de granskade myndigheterna.

3 Vad kostar det?

Syftet med denna granskning har varit att kunna uttala oss om myndigheterna utifrån dagens krav och förutsättningar bedriver ett informationssäkerhetsarbete, så att de uppnår ett ändamålsenligt skydd av sina informationstillgångar. En aspekt av ändamålsenligheten är att bedöma om myndigheterna gör effektiva avvägningar mellan investeringar i säkerhet och de risker som finns. För att kunna göra en sådan bedömning krävs dels uppgifter om myndigheternas kostnader för informationssäkerhet, dels uppgifter om eventuella risker. Detta kapitel behandlar myndigheters IT-kostnader på en övergripande nivå samt en kompletterande informationsinsamling som Riksrevisionen har låtit Radar Ecosystem Specialists göra, eftersom de granskade myndigheterna haft svårt att redogöra för sina kostnader för informationssäkerhet.

3.1 Vad visste vi före granskningen?

Frågan om omfattningen och redovisningen av myndigheternas IT-kostnader har berörts i ett flertal publikationer från slutet av 1990-talet och framåt. Trots det finns det ännu inte några säkra uppgifter om IT-kostnader i staten. ESV fick i regleringsbrevet för 2014 i uppdrag av regeringen att utveckla en modell för beräkningar av myndigheternas IT-kostnader och IT-investeringar i syfte att effektivisera användningen av IT, skapa jämförbarhet samt möjlighet till överblick och återanvändbarhet. ESV konstaterar i sin rapport att det i dag varken med stöd av myndigheternas extern- eller internredovisning går att mäta IT-kostnader på ett strukturerat sätt. I statsredovisningssystemet Hermes samlas utfallet för myndigheternas externredovisning in på så kallade S-koder. Externredovisningen utgår från kostnader för personal, lokaler, övrig drift samt ned- och avskrivningar. IT-kostnader ryms inom samtliga dessa, samtidigt som det inte finns några krav på att särredovisa IT-kostnader. Myndigheterna har inte heller tillgång till några gemensamma verktyg för att enkelt och effektivt kunna följa sina kostnader över tiden eller jämföra sig med andra myndigheter. Det gör det svårt att bedöma om IT används effektivt, både för myndighetsledningar och för regeringen.[70]

3.2 Varför behöver vi veta kostnaderna?

För att kunna göra en optimal avvägning av hur mycket vi som samhälle behöver skydda oss måste vi kunna relatera kostnaden för att skydda oss mot den nytta vi uppnår genom att skydda oss. Ett sätt att göra det är att analysera kostnaderna för

[70] Ekonomistyrningsverket: *IT-kostnadsmodell – ett första steg mot ett gemensamt språk* (ESV 2014:50), s. 10 och 17.

IT-händelser då dessa visar var kostnaderna uppstår, vilket kan vara alltifrån den drabbade organisationen till individer och skattebetalare i samhället.[71] Det finns i dag inte någon tillförlitlig sammanställning av de totala kostnaderna för otillgänglighet hos IT-system i Sverige. Ofta uppskattar man inte ens kostnaderna på medialt uppmärksammade händelser. Svårigheten att göra uppskattningar är också, enligt MSB, ett symptom på ett djupare problem: att de flesta organisationer inte vet hur sårbara de är. De vet inte vad driftavbrott kan komma att kosta när de gör sin riskhantering, och de har till och med i efterhand svårt att beräkna kostnaderna för inträffade driftavbrott.[72] Om det saknas sakligt underbyggda underlag för kostnader påverkas förmågan att etablera optimal säkerhet negativt ur ett totalt ekonomiskt perspektiv – såväl samhällsekonomiskt som företagsekonomiskt. Avsaknaden av tillräckliga underlag när det gäller kostnader försvårar för myndighetsledningarna att motivera utgifter för att reducera risk. En konsekvens av det kan bli att ledningar underfinansierar arbetet med riskreducering.

FOI anger i en rapport om informationssäkerhet och ekonomi att en stor del av forskningslitteraturen på området är av teoretisk karaktär och att det finns en märkbar avsaknad av utvärderingar av teoriernas praktiska tillämpbarhet. Det vore därmed enligt FOI angeläget att empiriskt undersöka vidare hur beslut om investeringar i informationssäkerhet görs i praktiken i dag, vilka faktorer som inkluderas i bedömningar och vilka metoder som används. Det vore enligt FOI även relevant att undersöka vilka organisatoriska faktorer som kan spela in för synen på investeringar i informationssäkerhet och hur arbetet på området praktiskt går till.[73] Den typen av uppgifter finns i andra länder som exempelvis Storbritannien där det regelbundet genomförs enkätundersökningar om informationssäkerhet. Undersökningarna berör bland annat kostnader för intrång och skydd, metoder för investeringar samt kontroll. För 2012 uppskattades den genomsnittliga kostnaden för skydd mot intrång vara cirka 8 procent av olika organisationers IT-budget (11 procent i de fall där säkerhet är prioriterat).[74]

För att öka kunskapen om hur det ser ut i Sverige finansierade MSB under 2014 ett projekt med uppdrag att undersöka kostnader för IT-incidenter i samhället. Målet med projektet var att bidra med ett ekonomiskt resonemang, så att fler aktörer kan arbeta systematiskt med säkerhet i sina IT-system för att uppnå en samhällsekonomiskt effektiv informationssäkerhet. Studien skulle även översiktligt beskriva befintliga kostnadsberäkningsmodeller för IT-incidenter på dels samhällsnivå, dels organisationsnivå. Projektet har arbetat med ett antal fallstudier över inträffade incidenter i syfte att visa hur en värdering skulle kunna ha gjorts, om det hade funnits

71 Branzell, Egnell, Kopsch, Norrström och Wilhelmsson: *Kostnader för IT-incidenter i samhället*, Stockholm 2014, s. 2.

72 MSB: *Informationssäkerhet – trender 2015*, s. 50–51.

73 Hermelin, Karlzén och Nilsson: *Informationssäkerhet och ekonomi* (FOI-rapport 3927), 2014, s. 50.

74 Hermelin, Karlzén och Nilsson, *Informationssäkerhet och ekonomi* (FOI-rapport 3927), 2014, s. 51.

tillförlitlig information om samhällsekonomiska värderingar av externa effekter. Även om projektet har syftat till att finna relevanta uppskattningar för kostnader för IT-incidenter kunde man konstatera att det saknades på de flesta områden. Man kunde även konstatera att det är viktigt att kunna ta ett steg till och med hjälp av samhällsekonomiska kalkyler beräkna huruvida investeringar för att minska antalet incidenter är önskvärda eller ej. För att kunna göra det behövs ytterligare kunskap och metoder för att på ett sakligt sätt mäta samhällsekonomiska kostnader av störningar i IT-system.[75]

Vad Riksrevisionen erfar har MSB inte tagit något initiativ till fortsättning på denna studie fram till dags dato.

3.3 Vad visade ESV:s rapport?

Som ovan nämnts fick ESV i regleringsbrevet för 2014 i uppdrag av regeringen att utveckla en modell för beräkningar av myndigheternas IT-kostnader och IT-investeringar. Syftet var att effektivisera användning av IT, skapa jämförbarhet samt ge möjlighet till överblick och återanvändbarhet.

ESV fick i januari 2015 i uppdrag av regeringen att fördjupa arbetet med jämförelser och även att fördjupa analysen av skillnader mellan olika myndigheter. ESV skulle även utarbeta förslag till regeringen på hur mätning och rapportering av de statliga myndigheternas IT-användning kan utvecklas och hur statsförvaltningens digitalisering kan följas upp. Detta kan bland annat omfatta hur statliga myndigheter ska mäta och rapportera effektiviteten i användningen av IT, IT-kostnader, strategiska IT-projekt och projekt med hög risk.[76]

ESV anför, som utgångspunkt för uppdraget, att det är rimligt utifrån kraven på intern styrning och kontroll i staten att myndighetsledningarna gentemot regeringen kan verifiera effektiviteten i myndighetens IT-verksamhet och redovisa, bedöma och motivera sin resursanvändning för IT i förhållande till annan verksamhet. Det handlar enligt ESV om att ha kunskap om den nytta som IT bidrar med i förhållande till vad det kostar, i första hand i den egna verksamheten men även i jämförelse med annan verksamhet. För att detta ska vara möjligt krävs ett gemensamt språk.[77]

I sitt arbete med uppdraget gjorde ESV, utöver att ta fram ett antal nyckeltal kopplade till IT-kostnader, också en kompletterande mätning av mognad inom inform-

---

[75] Branzell, Egnell, Kopsch, Norrström och Wilhelmsson: *Kostnader för IT-incidenter i samhället*, Stockholm 2014, s. 4.

[76] Regeringsbeslut 2015-01-15, N2015/738/EF: *Uppdrag att fördjupa arbetet med jämförelser av it-kostnader och att kartlägga it-projekt med hög risk*.

[77] Ekonomistyrningsverket: Fördjupat it-kostnadsuppdrag, delrapport 2 – *Kartläggning av it-kostnader* (2015:58), s. 10.

ationssäkerhet. Mätningen var inriktad mot intern styrning och kontroll av IT-verksamhet. ESV:s övergripande slutsats i rapporten är att myndigheternas interna styrning och kontroll av IT behöver utvecklas och stärkas. Ett första steg är att tydliggöra kraven på intern styrning och kontroll inom IT. ESV konstaterade att

- knappt hälften av myndigheterna har en aktuell och fungerande strategi för sin IT-försörjning
- 15 procent av myndigheterna saknar helt en IT-försörjningsplan
- bara knappt en tredjedel av myndigheterna har en styrning av processer inom förvaltning av system och projekt (portföljstyrning[78]) som används fullt ut
- endast 17 procent av myndigheterna har en beslutad modell för nyttohemtagning som efterlevs.[79]

ESV:s rapport innehåller förvisso ett antal nyckeltal för IT-kostnader överlag, dock inte för informationssäkerhet eller IT-säkerhet. Det finns alltså inte några uppgifter som möjliggör jämförelser mellan kostnader för informationssäkerhet eller IT-säkerhet i statsförvaltningen.

3.4 Vilka uppgifter har granskade myndigheter kunnat lämna?

Riksrevisionen har i denna granskning begärt uppgifter från de tre särskilt granskade myndigheterna om deras budget för arbete med informationssäkerhet under 2014 och 2015. En av myndigheterna har tagit fram delar av vad Riksrevisionen har efterfrågat i form av budget för vissa projekt om informationssäkerhet och för säkerhetsstabens verksamhet. De andra två myndigheterna har inte kunnat förete något budgetmaterial eller kunnat uppvisa kostnader för arbetet med informationssäkerhet. Den ena myndigheten svarade följande på Riksrevisionens begäran:

”Det finns ingen separat budgetering för enbart informationssäkerhet. Anledningen till detta är att arbetsområdet grenar ut över hela myndigheten och det i kombination med komplexiteten i frågorna, gör det omöjligt att med säkerhet säkerställa budgetsiffrorna. Vidare är det en definitionsfråga vad som innefattas inom begreppet informationssäkerhet, vilket ytterligare försvårar. Möjligtvis att det går att påvisa ett antal individers involvering och kostnaden för dessa. Vi ser dock inget mervärde av en ej fullständig analys, då vi inte kommer att kunna ge en komplett återspegling av verksamheten.”

[78] pm3 är en förvaltnings- och portföljstyrningsmodell som används dels för enskilda förvaltningsuppdrag, dels för att hantera en organisations totala uppdragsportfölj när det gäller förvaltning och utveckling.

[79] Ekonomistyrningsverket: Fördjupat it-kostnadsuppdrag, delrapport 2 – *Kartläggning av it-kostnader* (2015:58), s. 6.

Myndigheterna har således svårt att få fram en heltäckande bild av vilka resurser som läggs på informationssäkerhet.

3.5 Vad har den kompletterande informationsinsamlingen visat?

Det saknas i dag uppgifter om myndigheters kostnader för informationssäkerhet, såväl för var myndighet för sig som för statsförvaltningen i sin helhet. Exempelvis kunde endast en av de djupt granskade myndigheterna förete delar av de uppgifter om budget för informationssäkerhetsarbete som Riksrevisionen har efterfrågat. Denna granskning visar alltså att myndigheter har svårt att visa upp en heltäckande bild av vilka resurser som läggs på informationssäkerhet. Riksrevisionen har därför uppdragit åt en konsult[80] att undersöka kostnader för informationssäkerhet för statliga myndigheter. I detta kapitel redogör vi kortfattat för resultatet av denna undersökning. För att ta del av undersökningen i sin helhet hänvisar vi till elektronisk bilaga 4, som finns tillgänglig på Riksrevisionens webbplats www.riksrevisionen.se.

Undersökningen avser totalkostnader för proaktivt informationssäkerhetsarbete för tre anonymiserade statliga myndigheter.[81] Reaktiva kostnader, det vill säga kostnader som uppstår när en händelse väl har inträffat, ingår inte i undersökningen då incidenter som rör informationssäkerhet varierar både i grad och komplexitet och därför inte går att beräkna på ett rättvisande sätt. Den proaktiva totalkostnaden är beräknad utifrån en modell som tar hänsyn till nedlagd arbetstid som på olika sätt kan hänföras till informationssäkerhet samt löpande kostnader för IT-säkerhetsteknik och externa IT-tjänster. Riksrevisionen bedömer att modellen skulle kunna vara en utgångspunkt för att dela upp kostnader för informationssäkerheten på olika delar av en myndighet. Diagram 3.1 på motstående sida visar översiktligt hur modellen är uppbyggd.

[80] Radar Ecosystem Specialists.

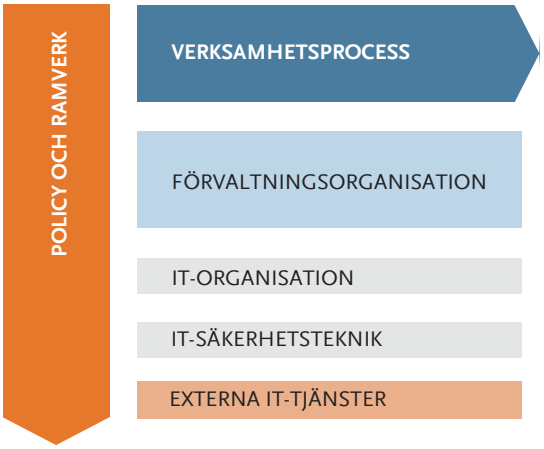
[81] Dessa myndigheter är inte någon av de övrigt granskade myndigheterna.

Diagram 3.1 Modell för beräkning av kostnader för informationssäkerhet

Nedlagd arbetstid på informationssäkerhetsarbete för personal i olika befattningar och roller, som är involverade i informationssäkerhetsarbete för att ta fram, efterleva och utvärdera policy, ramverk och processer. Denna arbetstid återfinns framför allt inom verksamhetsprocesser, förvaltningsorganisation och IT-organisation.

Kostnader för IT-säkerhetsteknik som kan härledas till system och applikationer som anskaffats i syfte att säkra verksamhetens information.

Kostnader för externa IT-tjänster som går att härleda till tjänster i syfte att säkra verksamhetens information.



Källa: Radar Ecosystem Specialists

Undersökningen har visat att kostnaderna för proaktivt informationssäkerhetsarbete för de statliga myndigheter som ingått i undersökningen i genomsnitt uppgår till 24,7 miljoner kronor per verksamhet och år. Därav utgör IT-säkerhetsteknik den allra största delen, 16,5 miljoner kronor, motsvarande 67 procent. Externa IT-tjänster uppgår till 2,5 miljoner kronor, vilket motsvarar 10 procent. Nedlagd arbetstid hänförlig till informationssäkerhet uppgår till 5,6 miljoner kronor, motsvarande 23 procent. Sammanlagt står IT-säkerhetsteknik och externa IT-tjänster för mer än tre fjärdedelar av kostnaderna för informationssäkerheten vid de undersökta myndigheterna.

Den genomsnittliga kostnaden för proaktivt informationssäkerhetsarbete – 24,7 miljoner kronor – motsvarar 16 367 kronor per sysselsatt. Skillnaderna mellan de undersökta myndigheterna är dock stor; kostnaden varierar mellan 13 809 och 29 159 kronor.[82] Av tabell 3.1 på nästa sida framgår hur den genomsnittliga kostnaden fördelar sig inom myndigheterna.

[82] Detta beror på deras skilda uppdrag och storlek, vilket innebär att de genomsnittliga kostnaderna för proaktiv informationssäkerhet snarare bör betraktas som en orientering än en exakt jämförelse.

Tabell 3.1 Fördelning av den genomsnittliga kostnaden 16 367 kronor per sysselsatt och år

Del av verksamhet	Kronor
Kärnverksamhet	897
Förvaltning och utveckling	597
IT-organisation	2 254
IT-säkerhetsteknik	10 932
Externa IT-tjänster	1 687

Källa: Radar Ecosystem Specialists.

4 Har regeringen skapat tillräckliga förutsättningar?

Arbetet med informationssäkerhet på myndigheterna ligger inom ramen för det som kallas intern styrning och kontroll. Intern styrning och kontroll är en process som syftar till att en myndighets ledning ska se till att verksamheten bedrivs effektivt och rättsenligt, att den redovisas tillförlitligt och rättvisande samt att man hushållar väl med statens medel.[83]

4.1 Vad har regeringen gjort?

Regeringen har utfärdat förordningar som syftar till att främja intern styrning och kontroll i statsförvaltningen: myndighetsförordningen och förordningen om intern styrning och kontroll. Även internrevisionsförordningen (2006:1228) syftar till detta. Regeringen har även bemyndigat MSB att utfärda föreskrifter inom området informationssäkerhet.[84] Detta innebär att regeringen har delegerat ansvaret till myndigheternas ledningar i fråga om intern styrning och kontroll och till MSB när det gäller bestämmelser om ledningssystem för informationssäkerhet.

Trots att ansvaret för intern styrning och kontroll ligger på respektive myndighets ledning har ändå regeringen ett ansvar för att styra myndigheterna. Denna styrning utövas av respektive myndighets huvudman i det departement myndigheten lyder under. Vi har i denna granskning undersökt i vad mån informationssäkerhet är föremål för styråtgärder gentemot de tre särskilt ingående granskade myndigheterna Arbetsförmedlingen, Försäkringskassan och Migrationsverket.[85]

4.1.1 Frågor om informationssäkerhet har varit aktualiserade

Frågor om informationssäkerhet har aktualiserats i Regeringskansliet för alla tre myndigheter under perioden 2015 fram till mitten av februari 2016. Det har skett på olika sätt. En myndighet har i årsredovisningen för 2014 bedömt att den interna styrningen och kontrollen hade brister i beredskapen för att hantera störningar i kritiska IT-system. För en annan myndighet har saken aktualiserats genom myndighetens risk- och sårbarhetsanalys. För en tredje myndighet har det skett genom att Riksrevisionen granskat en viss typ av ärendehandläggning.[86]

---

83 3 § myndighetsförordningen (2007:515) samt 2 § förordningen (2007:603) om intern styrning och kontroll.

84 34 § förordningen (2006:942) om krisberedskap och höjd beredskap.

85 Svar på skriftliga frågor ställda till huvudmännen för Arbetsförmedlingen, Försäkringskassan och Migrationsverket inkomna till Riksrevisionen den 17 och 18 februari 2016.

86 Svar på skriftliga frågor ställda till huvudmännen för Arbetsförmedlingen, Försäkringskassan och Migrationsverket inkomna till Riksrevisionen den 17 och 18 februari 2016.

En förutsättning för att Regeringskansliet ska agera är att man blir underrättad av sin myndighet om sakernas tillstånd. Om en myndighet inte har redovisat något i fråga om intern styrning och kontroll av informationssäkerhet har Regeringskansliet inte vidtagit några åtgärder. Utöver vad som rapporterats i årsredovisningen för de tre särskilt djupt granskade myndigheterna är det inte mycket som myndigheterna informerar sina departement om när det gäller intern styrning och kontroll av informationssäkerheten. Två av departementen har inte heller efterfrågat någon information från myndigheten om dess interna styrning och kontroll av informationssäkerheten. Ett av departementen har uppgett att man har uppmanat sin myndighet att tydligare redovisa, konkretisera och mer tydligt definiera eventuella brister i informationssäkerheten i risk- och sårbarhetsanalysen. Detta skedde eftersom myndigheten i sin årsredovisning bedömt att informationssäkerheten, enligt modellen för intern styrning och kontroll, var bristfällig. Myndigheten redovisade sedan en risk- och sårbarhetsanalys som innehöll en mer detaljerad och omfattande beskrivning av informationssäkerheten. Övriga åtgärder som vidtagits i Regeringskansliet till följd av det som myndigheterna redovisat är främst att ta upp saken i den dialog som förs med myndigheten (två myndigheter), och i ett fall gav regeringen också i uppdrag till Statskontoret att analysera den interna styrningen och utvecklingsarbetet på en av myndigheterna.[87]

4.1.2 Regeringen skulle kunna ställa mer krav

Ansvariga för informationssäkerheten vid två av de sex granskade myndigheterna anser att deras departement skulle kunna lämna mer stöd, inte minst i form av att ställa tydliga krav på säkerheten. En av de sex granskade myndigheterna anser att stödet är gott. Hur säkerhetsansvariga vid de övriga myndigheterna uppfattar stödet från sina departement har det inte gått att få någon entydig bild av.[88] Det hänger naturligen samman med att det kan vara ganska långt mellan de ansvariga för informationssäkerheten och respektive departement.

Finansdepartementet har också en roll i fråga om intern styrning och kontroll av informationssäkerheten. Finansdepartementet anordnar utbildning om de regelverk som styr intern styrning och kontroll för myndighetshandläggarna i Regeringskansliet. Dessutom har Finansdepartementet tagit initiativ till att fackdepartementen ska arbeta mer med frågor som rör intern styrning och kontroll vid styrningen av myndigheterna.[89] Två av de här aktuella fackdepartementen har uppgett att de är nöjda med det stöd de får, från såväl Finansdepartementet som ESV, när det gäller intern styrning och kontroll av informationssäkerhet. Ett av fackdepartementen

---

87 Svar på skriftliga frågor ställda till huvudmännen för Arbetsförmedlingen, Försäkringskassan och Migrationsverket inkomna till Riksrevisionen den 17 och 18 februari 2016.

88 Intervjuer på de sex myndigheterna.

89 Intervjuer på Finansdepartementet den 9 december 2015.

uppger dock att det saknas stöd för vilken redovisning som bör efterfrågas och vilken nivå på informationssäkerheten som bör vara rimlig.[90]

4.1.3 Regeringen har dock ställt vissa krav på redovisning

Till följd av Riksrevisionens tidigare granskning av informationssäkerhet i statsförvaltningen[91] beslutade regeringen att i regleringsbrev för 2015 ge ett uppdrag till de myndigheter som har ett särskilt ansvar för krisberedskapen[92]. Syftet var att regeringen skulle få en bättre lägesbild genom att myndigheterna i sin redovisning av arbetet med risk- och sårbarhetsanalys särskilt lyfter fram arbetet med informationssäkerhet.[93] Uppdraget innebar att myndigheterna i arbetet med 2015 års risk- och sårbarhetsanalyser skulle särskilt beakta och analysera informationssäkerheten i de delar av verksamheten och i de tekniska system som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. I detta arbete skulle även informationssäkerheten inom myndigheternas ansvarsområde beaktas och analyseras. Myndigheterna skulle redovisa en bedömning av informationssäkerheten samt vilka åtgärder som är vidtagna.[94] Det var således 45 myndigheter som fick detta uppdrag: 24 centrala myndigheter samt de 21 länsstyrelserna.[95] Urvalet av myndigheter som fick i uppdrag att särskilt beakta och analysera informationssäkerheten omfattade endast de som har ett särskilt ansvar för krisberedskapen, vilket fick till följd att andra myndigheter som har särskilt skyddsvärd information inte kom att omfattas av uppdraget.

4.2 Vad har ESV gjort?

ESV har regeringens uppdrag att bistå med det underlag regeringen behöver för att säkerställa att statsförvaltningen är effektiv och att den interna styrningen och kontrollen är betryggande.[96]

ESV utför sitt uppdrag att bistå regeringen genom att årligen gå igenom årsredovisningar. ESV tar då del av de bedömningar om den interna styrningen och kontrollen är betryggande som ledningen, vid de myndigheter som omfattas av förordningen

90 Svar på skriftliga frågor ställda till huvudmännen för Arbetsförmedlingen, Försäkringskassan och Migrationsverket inkomna till Riksrevisionen den 17 och 18 februari 2016.

91 Informationssäkerheten i den civila statsförvaltningen (RiR 2014:23).

92 Enligt 9 § tredje stycket förordningen (2006:942) om krisberedskap och höjd beredskap.

93 Svar på skriftliga frågor ställda till huvudmännen för Arbetsförmedlingen, Försäkringskassan och Migrationsverket inkomna till Riksrevisionen den 17 och 18 februari 2016.

94 Likalydande uppdragsbeskrivning i 2015 års regleringsbrev till de områdesansvariga myndigheterna enligt 11 § förordningen (2006:942) om krisberedskap och höjd beredskap.

95 Enligt bilaga till förordningen (2006:942) om krisberedskap och höjd beredskap med förteckning över samverkansområden och myndigheter som har särskilt ansvar inom områdena.

96 2 § 1 förordningen (2010:1764) med instruktion för Ekonomistyrningsverket.

om intern styrning och kontroll, ska göra i anslutning till underskriften i årsredovisningen.[97] Det rör sig för 2015 om bedömningar från 67 myndigheter som tillsammans svarar för huvuddelen av utgifterna på statsbudgeten. Till detta kommer att ESV årligen kontrollerar hur myndigheter efterlever de regler som finns på det ekonomiadministrativa området (EA-värdering). ESV undersöker också årligen efterlevnad av intern styrning och kontroll genom en enkätundersökning av internrevisionen vid de 67 myndigheter som har en sådan.[98] Allt detta rapporteras också publikt.

ESV:s uppdrag har således en stödjande karaktär, inte övervakande. Det fulla ansvaret att se till att den interna styrningen och kontrollen är betryggande ligger på respektive myndighets ledning. Därför har ESV, förutom de ovan beskrivna åtgärderna, inte heller närmare följt upp den interna styrningen och kontrollen på myndigheter i statsförvaltningen.

Statskontoret gjorde 2015 en analys av ESV. I den framkommer att myndigheter efterfrågar mer stöd från ESV när det gäller intern styrning och kontroll och att bedöma risker. Myndigheterna uttrycker att det behövs mer konkret handledning.[99] Finansdepartementet instämmer i vad Statskontoret anfört om ESV. Samtidigt har ESV efterfrågat en större tydlighet från regeringen när det gäller frågor om intern styrning och kontroll. ESV har enligt Finansdepartementet inte tillräcklig insyn i tillståndet på respektive myndighet, och borde kanske kunna göra fler insatser för att främja en betryggande intern styrning och kontroll i statsförvaltningen.[100] Som framgår av föregående kapitel saknas det en samlad bild av de kostnader som statsförvaltningen lägger ned på informationssäkerhet, vilket är en bristande förutsättning för de avvägningar som behöver göras mellan kostnader och nytta.

---

97 Enligt 2 kap. 8 § förordningen (2000:605) om årsredovisning och budgetunderlag.

98 Intervjuer på Ekonomistyrningsverket 2015-12-01.

99 Statskontoret (2015:15): *Myndighetsanalys av Ekonomistyrningsverket*, s. 64.

100 Intervju på Finansdepartementet den 9 december 2015.

Referenser

Författningar

Budgetlagen (2011:203)

Myndighetsförordningen (2007:515)

Förordningen (2000:605) om årsredovisning och budgetunderlag

Förordningen om intern styrning och kontroll (2007:603)

Förordningen (1995:1300) om statliga myndigheters riskhantering

Förordningen (2006:942) om krisberedskap och höjd beredskap

Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

Säkerhetsskyddsförordningen (1996:633)

MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10)

MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2015:3)

Offentligt tryck

Departementspromemoria: Intern styrning och kontroll i staten (Ds 2006:15)

Ekonomistyrningsverket: IT-kostnadsmodell – Ett första steg mot ett gemensamt språk (2014:50)

Ekonomistyrningsverket: Fördjupat it-kostnadsuppdrag, delrapport 2 – Kartläggning av it-kostnader (2015:58).

Myndigheten för samhällsskydd och beredskap: Informationssäkerhet – trender 2015

Regeringsbeslut 2015-01-15 (N2015/738/EF): Uppdrag att fördjupa arbetet med jämförelser av it-kostnader och att kartlägga it-projekt med hög risk

Riksrevisionen: Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen (RiR 2007:10)

Riksrevisionen: Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten (promemoria 2005, dnr 31-2004-1295)

Riksrevisionen: Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten (RiR 2005:27)

Riksrevisionen: Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten (RiR 2006:24)

Riksrevisionen: Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten (RiR 2006: 25)

Riksrevisionen: Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten (RiR 2006:26)

Riksrevisionen: Bolagsverkets informationssäkerhet (promemoria 2005, dnr 32-2005-0717)

Riksrevisionen: Granskning av Försäkringskassans interna styrning och kontroll av informationssäkerheten (revisionsrapport 2006, dnr 32-2005-0655)

Riksrevisionen: Post- och telestyrelsens informationssäkerhet (revisionsrapport 2006, dnr 32-2005-0738)

Riksrevisionen: Löpande granskning av Affärsverket Svenska Kraftnät 2005 (revisionsrapport 2006, dnr 32-2005-0714)

Riksrevisionen: Försvarsmaktens styrning av informationssäkerhetsarbetet (revisionsrapport 2006, dnr 32-2005-0551)

Riksrevisionen: Löpande granskning av Affärsverket Svenska Kraftnät 2006 (revisionsrapport 2007, dnr 32-2006-0700)

Riksrevisionen: Informationssäkerheten i den civila statsförvaltningen (RiR 2014:23)

Statskontoret: Myndighetsanalys av Ekonomistyrningsverket (2015:15)

Övriga tryckta källor

Branzell, Egnell, Kopsch, Norrström och Wilhelmsson: Kostnader för IT-incidenter i samhället (Stockholm, 2014)

Hermelin, Karlzén och Nilsson: Informationssäkerhet och ekonomi (FOI-rapport 3927), 2014

Radar Ecosystem Specialists: IT- och informationssäkerhet – statliga myndigheter och verk, 2015–2016

Otryckta källor

Enkätundersökning i november 2015 till Affärsverket svenska kraftnät, Bolagsverket, Lantmäteriet, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk

Interna regler, riktlinjer, policyer, m.m. vid de granskade myndigheterna

Minnesanteckningar från ledningsgruppsmöten vid de granskade myndigheterna

Protokoll från styrelsemöten vid de granskade myndigheterna

Bilaga 1. Förklaringar till ord och begrepp

Här följer förklaringar till de särskilda ord och begrepp som används i rapporten.

Behörighet – Med behörighet avses av systemansvarig tilldelad rättighet till system. Behörighet kan bestå av olika nivåer som till exempel endast läsrättighet, rätt att registrera och rätt att radera. Behörigheten kopplas till ett användarkonto.

Behörighets- och kontrollsystem – Med behörighetskontrollsystem (BKS) avses ett system som administrerar användarkonton och tilldelar åtkomst till material och funktioner i ett verksamhetssystem. BKS verifierar behörig användare genom att kontrollera användarens användarkonto och i detta registrerat lösenord mot det lösenord som användaren anger vid inloggning. Exempel på BKS som kan ingå i en användares inloggning är arbetsplatsens, nätverkets, applikationsserverns, databasserverns och databashanterarens. BKS-rättigheter ger användare rätt att använda en funktion i systemet. Detta kan exempelvis innefatta rättigheter att skapa ärenden, skapa dokument, redigera dokument, m.m. Behörighet tilldelas till enskilda dokument, mappar och ärenden för att ange vilka användare som ska få läsa dessa och vilka användare som ska få behörighet att redigera dem.

Datamedia – Bärare av information i form av hårddiskar, databand, disketter, usbminnen eller liknande.

Eskalering – Att föra upp en risk på en högre organisatorisk nivå för beslut om huruvida risken ska hanteras och i så fall hur. Att man eskalerar en risk kan bero på att man inte har tillräckliga resurser eller möjligheter att hantera den på ifrågavarande organisatoriska nivå eller att risken är delad på flera ställen i organisationen eller förekommer på många olika ställen i organisationen.

Externredovisning – Den externa redovisningen omfattar bokföring, årsredovisning och i vissa fall även koncernredovisning. Den ska främst utmynna i en resultaträkning och en balansräkning per år, och i vissa fall även i en kassaflödesanalys.

Fjärranslutning – En teknik för fjärråtkomst som möjliggör att anställda kan komma åt sina e-postkonton och delade filer hemifrån eller på andra platser utanför företagets nätverk via internet.

Gruppidentiteter – En användaridentitet i systemet som inte är kopplad till en enskild person.

Informationsägare – Informationsägare är den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt genom vilket informationen sprids. Informationsägaren formulerar dels icke-funktionella krav som tillgänglighet, kapacitet, säkerhetsnivå, dels funktionella krav som på vilket sätt information ska visas och vilken information som ska finnas. Informationsägaren är därmed riskägare för den information som ska hanteras.

Incident – Oönskad och oplanerad händelse som kan påverka en organisation och som kan innebära en störning av organisationens förmåga att bedriva sin verksamhet.

Incidentrapportering – Rutin för att rapportera incidenter i verksamheten. Syftet med rapporteringen är att skapa en erfarenhetsbank och underlag för förbättringsåtgärder

Informationstillgångar – Med informationstillgångar avses verksamhetens information och tillgångar relaterade till informationshantering, såsom IT-system, medarbetare, Internetkapacitet, etc.

Internredovisning – Intern redovisning används bland annat för framtagande och uppföljning av budgetar och ekonomiska kalkyler samt av rapporter som används löpande under året. Till skillnad från den externa redovisningen finns det ingen lagstiftning som reglerar hur den interna redovisningen ska utformas eller vad den ska omfatta.

Intrångstest (PEN-test) – Tekniska sårbarhetsanalyser eller så kallade penetrationstester är ett vedertaget sätt att skanna IT-system eller nätverk i syfte att upptäcka kända brister och svagheter i IT-systemen som kan bli kritiska för verksamheten.

ISO 27000 – ISO/IEC 27000-serien är en samling säkerhetsstandarder utgivna av standardiseringsorganisationerna ISO och IEC. I Sverige är beteckningen för serien SS-ISO/IEC 27000. Standarderna i ISO/IEC 27000-serien är verktyg som en organisation kan välja att utgå ifrån i arbetet med informationssäkerhet. Standarderna kan ge en organisation riktlinjer för hur risker och hot kan kartläggas och hanteras på ett systematiskt sätt. Standardserien omfattar ledningens ansvar, administrativa rutiner och övergripande krav på IT-infrastruktur. Det finns möjlighet till oberoende certifiering av informationssäkerheten, i likhet med standarder för kvalitet ISO 9000 och miljö ISO 14000. I Sverige bedrivs utvecklingen av SIS, Swedish Standards Institute.

IT-incident – en oönskad och oplanerad IT-relaterad händelse som kan påverka säkerheten i en organisations eller samhällets informationshantering, och som kan innebära en störning i förmågan att bedriva en verksamhet.

Kontinuitetsplanering – En metod för att säkerställa organisationens leveransförmåga genom att planera för fortsatt verksamhet vid förlust av operativ förmåga. Det vill säga att trots avbrott kunna leverera de tjänster eller produkter som är viktigast för organisationen och dess avnämare.

Kärnverksamhet – En myndighets verksamhet brukar delas upp i kärnverksamhet och stödverksamhet. Det finns ingen given definition av vad som ska betraktas som kärnverksamhet (och följaktligen inte heller av vad som ska betraktas som stödverksamhet). Statlig kärnverksamhet kan definieras som den verksamhet som en myn-

dighet bedriver enligt lagar, förordningar och andra styrdokument. Stödverksamheten utgörs av det stöd i olika avseenden som ges för att kärnverksamheten ska kunna bedrivas. I denna rapport hanteras säkerhetsstab, IT-avdelning och liknande funktioner som stödverksamhet.

Ledningssystem för informationssäkerhet (LIS) – Alla organisationer har ett ledningssystem, eller ett ”system” för att leda verksamheten. Det handlar helt enkelt om hur ledningen styr verksamheten. Detta ledningssystem kan vara mer eller mindre strukturerat och mer eller mindre konkret. Det kan kallas för styrsystem eller styrmodell eller ingenting alls, men det finns där. Ett ledningssystem för informationssäkerhet är den del av ledningssystemet som styr informationssäkerheten i verksamheten.

Prestandamätning – En analysmetod som mäter existerande säkerhetsnivå i förhållande till ett bör-läge, som utgår från såväl kraven i ISO 27000-standarden som i olika författningar. Metoden är generisk och fungerar på de flesta typer av verksamhet.

Revisionsloggar – Logg för att registrera användning, ändringar, statusförändring eller avvikelser i ett system.

Riskhantering – en process för att identifiera och hantera risker som omfattar riskanalys (definiera omfattning, identifiera risker, beskriva risker), riskvärdering (värdera om risken kan tolereras, analysera alternativ) och riskreduktion/kontroll (fatta beslut, åtgärda, följa upp).

S-koder – En kodstruktur för att samla in statliga myndigheters ekonomiska information i en enhetlig struktur i statsredovisningssystemet.

Skalskydd – Skalskydd är den gräns i ett utrymme, en lokal eller en fastighet som har ett fysiskt skydd vilket försvårar forcering och obehörigt tillträde. Uppdelning av skalskydd görs i mekaniskt skydd, elektroniskt skydd och bevakning.

Systemadministrativa behörigheter – Tillgång till rättigheter i ett system utöver vad vanliga användare har. Kan exempelvis bestå av rättighet att redigera systeminställningar, lägga upp och ändra behörighet på andra användare, m.m.

Tvåfaktorautentisering – identitetskontroll (autentisering) med hjälp av två skilda former av information, till exempel ett kort och ett lösenord.

VPN – Virtuellt privat nätverk. Teknik som används för att skapa en säker förbindelse eller "tunnel" mellan två punkter i ett icke-säkert datanätverk (till exempel internet). Exempel på användning av VPN-anslutningar är att någon på resande fot kopplar upp sig mot företagets server för att arbeta som om klienten vore ansluten i det lokala nätverket.

WLAN - Wireless Local Area Network. Ett trådlöst, lokalt datornätverk.

Bilaga 2. Översikt av mätområden för de djupt granskade myndigheterna

Denna bilaga beskriver översiktligt den struktur som gäller för de fördjupade granskningar som skett av informationssäkerhetsarbetet på Arbetsförmedlingen, Försäkringskassan och Migrationsverket.

När det gäller de andra granskade myndigheterna har utgångspunkten främst varit det som de tidigare granskningarna har visat. Det gör att strukturen inte i alla delar stämmer överens med de fördjupade mätningarna.

Organisation

Mätområdet Organisation består av följande kategorier.

Personal och informationssäkerhet

Kategorin Personal och informationssäkerhet omfattar bland annat medvetenhet om regler och förekomst av information och utbildning när det gäller informationssäkerhet.

Skalskydd

Kategorin Skalskydd omfattar hantering av besökare och passersystem.

Informationssäkerhetsledning

Kategorin Informationssäkerhetsledning omfattar ledningssystem för informationssäkerhet (LIS) samt ansvar och utvärdering av detsamma. Avsikten med kategorin är att granska om verksamheten är så organiserad att den förmår driva ett LIS.

Analys och kontroll

Syftet med kategorin Analys och kontroll är att granska om ett strukturerat säkerhetsarbete bedrivs med regelbundna kontroller och analyser, om det genomförs riskanalyser samt om kontinuitetsplanering sker i tillräcklig omfattning.

Informationstillgångar

Kategorin Informationstillgångar omfattar klassificering av informationstillgångarna och dylikt. Syftet är att granska om myndigheten har kontroll över väsentliga informationstillgångar genom bland annat applikationer, databaser samt nyckelpersoner.

Incidenthantering

Syftet med kategorin Incidenthantering är att bedöma förmågan att kunna hantera och följa upp incidenter och omfattar såväl själva hanteringen som hur den är organiserad.

Ledningens styrande dokumentation

Syftet med kategorin Ledningens styrande dokumentation är att undersöka om det finns ett ramverk av styrande dokument för informationssäkerhetsarbetet.

System (IT)

Mätområdet System (IT) består av följande kategorier.

Behörigheter och kontrollsystem

Kategorin Behörigheter och kontrollsystem omfattar säker hantering av lösenord och dokumentation av behörigheter.

Spårbarhet

Kategorin Spårbarhet omfattar användaridentiteter och dokumentation av incidenter.

Ledningens styrande dokumentation

Kategorin Ledningens styrande dokumentation omfattar lösenordsdesign och regler för fjärranslutning av teknisk utrustning.

Riskhantering

Mätområdet Riskhantering är särskilt framtaget för Riksrevisionens granskning och är inte indelat i kategorier. Riksrevisionens syfte med mätområdet är att påvisa frekvensen av olika processer för riskhantering med utgångspunkt från tre av de författningar som innehåller bestämmelser om riskhantering: MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10), MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2015:3) samt förordningen om intern styrning och kontroll (2007:603).

Bilaga 3. Sammanställning av mätresultaten från de djupt granskade myndigheterna

Rubrik i rapporten	Delområden	Bedömning 1–5			Godkänt	Ej godkänt
2.1.1 Personal och infosäk		Mynd A	Mynd B	Mynd C		
	Anställningsrutiner	2	2	1		A B C
	Personal och informationssäkerhet	3	3	4	A B C	
	Regler för hantering av bärbar utrustning	3	1	4	A C	B
	Medvetenhet om regler för hantering av bärbar utrustning	2	1,8	1,9		A B C
	Info/utbildning om informationssäkerhet	2	2	1		A B C
	Installationsrutiner för mobiltelefoner och surfplattor	2	2	3	C	A B
	Informationsspridning gällande säkerhetsrelaterade hot	3	4	3	A B C	
2.1.2 Ledningens styrande dokumentation		Mynd A	Mynd B	Mynd C		
	Informationssäkerhetsdokument	1	0,38	0,6		A B C
	Hantering av information	2,5	1	2,1		A B C
	Informationssäkerhetspolicy	2	2	4	C	A B
	Riktlinjer för internetanvändning	1	1	0		A B C

Rubrik i rapporten	Delområden	Bedömning 1–5			Godkänt	Ej godkänt
2.1.3 Incidenthantering		Mynd A	Mynd B	Mynd C		
	Incidenthantering	1,57	1,75	1,67		A B C
	Incidentorganisation	3	2	2	A	B C
2.1.4 Informationstillgångar		Mynd A	Mynd B	Mynd C		
	Informationsklassning	3	3	3	A B C	
	Modell för informationsklassning	4	5	4	A B C	
	Överföring av krav på säkerhet från verksamhet till IT	0	0	1		A B C
	Ansvar för informationstillgångar	0	1	2		A B C
	Nyckelpersonsberoende	1	1	2		A B C
2.1.5 Analyser och kontroller		Mynd A	Mynd B	Mynd C		
	Kontinuitetsplanering	2	2	1		A B C
	Kontroll av IT-projekt	3	4	2	A B	C
	Välja säkerhetsåtgärder	2	2	0		A B C
	Riskanalys	2	2	2		A B C
2.1.6 Informationssäkerhetsledning		Mynd A	Mynd B	Mynd C		
	Ansvar LIS	3	3	3	A B C	
	Utvärdering LIS	2	2	2		A B C

Rubrik i rapporten	Delområden	Bedömning 1–5			God-känt	Ej god-känt
	Ledningens genomgång	0	0	0		A B C
2.1.7 Skalskydd		Mynd A	Mynd B	Mynd C		
	Besökande	4	4	3	A B C	
	Passersystem	4	5	4	A B C	
2.3.1 Behörighet och kontrollsystem		Mynd A	Mynd B	Mynd C		
	Administration av användaridentiteter	4	2	2	A	B C
	Dokumentation av behörigheter	2	2	2		A B C
	Verksamhetssystem Behörigheter - rättigheter	2	2	4	C	A B
	Säker lösenordshantering	1,12	0,78	1,5		A B C
2.3.2 Ledningens styrande dokumentation (system)		Mynd A	Mynd B	Mynd C		
	Verksamhetssystem Kontroll av åtkomst	3	1	2	A	B C
	Lösenordsdesign	0	2	3	C	A B
	Regler för fjärranslutning	5	5	5	A B C	
	Regler för säker utveckling	3	4	3	A B C	

Rubrik i rapporten	Delområden	Bedömning 1–5			God-känt	Ej god-känt
2.3.3 Spårbarhet och drift		Mynd A	Mynd B	Mynd C		
	Användaridentiteter	2	2	2		A B C
	Innehåll i revisionsloggar	2	2	2		A B C
	Dokumentation av incidenter	3	2	2	A	B C
	Reglering säkerhetsloggning	X	1	0		B C
	Verksamhetssystem Säkerhetskrav	3	3	3	A B C	
	Verksamhetssystem Kontinuitetsplanering	2	2	2		A B C
	Avveckling av datamedia	3	2	0	A	B C
	WLAN - Säkerhetsansvar	1	1	2		A B C
	Säkerhetskopiering	5	2	5	A C	B

Bilaga 4. Lista över roller för intervjupersoner vid de djupt granskade myndigheterna

IT-ansvarig
Den befattningshavare som har ansvar för IT-organisationen och därmed hårdvara, mjukvara och kommunikation i en myndighet. Normalt är denna roll IT-chef.

IT-säkerhetsansvarig
Den befattningshavare som har ansvar för bevaka IT-säkerhetsfrågor, det vill säga tekniska säkerhetsåtgärder i verksamhetens IT-system.

Informationssäkerhetsansvarig
Den befattningshavare som har ansvar för att driva informationssäkerhetsfrågor i myndigheten, framför allt rörande organisatorisk-administrativ säkerhet.

Driftansvarig IT
Den befattningshavare som är ansvarig för driften av myndighetens IT-system. I vissa myndigheter innehas denna roll av IT-chef eller motsvarande. I andra myndigheter är denna roll delegerad till annan medarbetare.

Informationsägare
Den befattningshavare som har ansvar för information som hanteras i ett för myndigheten viktigt verksamhetssystem (IT-system). Informationsägaren äger ansvar för sin verksamhet, därmed också för informationen och dess hantering. Informationsägarens viktigaste roll både vad gäller säkerhet och funktionalitet är att vara kravställare.

Systemägare
Den befattningshavare som är ansvarig för att funktionalitet och säkerhet hanteras i ett för myndigheten viktigt verksamhetssystem (IT-system), som motsvarar de krav verksamheten (informationsägaren) ställt.

Operativ ledning
Representant för myndighetens ledning, till exempel generaldirektör eller ställföreträdande generaldirektör. Kan också vara annan representant i en myndighets ledningsgrupp, dock ej IT-chef.

Myndighetsledning
Representant från myndighetens styrelse eller myndighetschef i en enrådigt styrd myndighet.

Personalansvarig
Den befattningshavare som har ett centralt ansvar för personal- och HR-frågor.

Säkerhetschef
Den befattningshavare som har ett övergripande säkerhetsansvar i myndigheten, det vill säga framför allt fysiskt skydd och personssäkerhet.

Internrevisor
Den befattningshavare som har till uppgift att granska den interna styrningen och kontrollen.

Linjechef
Den befattningshavare som har ett uttalat verksamhetsansvar, och därmed har ansvar för att hantera risker i sin verksamhet.

Riskanalysutförare för krisberedskapsområdet
Den befattningshavare som ansvarar för att genomföra riskanalyser i enlighet med förordningen (2006:942) om krisberedskap och höjd beredskap.[101]

Riskanalysutförare för området intern styrning och kontroll
Den befattningshavare som ansvarar för att genomföra riskanalyser i enlighet förordningen (2007:603) om intern styrning och kontroll.

Riskanalysutförare för informationssäkerhetsområdet
Den befattningshavare som ansvarar för att genomföra riskanalyser i enlighet med Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).[102]

Medarbetare
Medarbetare utan särskild kunskap om informationssäkerhet och som representerar användarperspektivet på olika nivåer i myndigheten.

---

[101] Sedan 1 april 2016 enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

[102] Sedan 4 april 2016 enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2016:1).