Granskning av Polismyndighetens informationssäkerhetsarbete

Internrevisionen – Marja Seppänen och Lars Agerberg

2018-11-28

Granskning av Polismyndighetens informationssäkerhetsarbete

INNEHÅLL

1 Sammanfattning

Granskningen har utförts i enlighet med revisionsplan för 2016-2017. Syftet med granskningen har varit att bedöma den interna styrningen och kontrollen av Polismyndighetens informationssäkerhetsarbete.
Granskningen har omfattat det myndighetsövergripande informationssäkerhetsarbetet. Efter att uppdragsbeskrivningen beslutades har internrevisionen gjort ytterligare en avgränsning avseende den del av informationssäkerheten som omfattar säkerhetsskyddet, även om det är en del av informationssäkerhetsarbetet. Skälet är att säkerhetsskyddsarbetet regleras av andra regelverk än MSB: s föreskrifter.

Intervjuer har genomförts med medarbetare från it- avdelningen och verksamhetsskyddet på RPCK, verksamhetsskydd vid två regionkanslier, NFC samt NOA. En analys av styrdokument och övriga beslut har även genomförts. En övergripande enkät skickades också till informationsägarna.

Internrevisionen anser att det finns risker förknippade med den interna styrningen och kontrollen beträffande det myndighetsövergripande informationssäkerhetsarbetet. Internrevisionens bedömning är att myndigheten inte har en ändamålsenlig process för styrning av informationssäkerhetsarbetet. Dels är processansvaret för informationssäkerhet delad mellan två funktioner, dels har styrningen av informationssäkerheten fördelats efter lagringsmedia/form och inte efter skyddsvärde och mål för myndighetens informationssäkerhet. Internrevisionen bedömer att för att de ska finnas förutsättningar för att upprätta och använda ett LIS som del av intern styrning och kontroll så behöver styrningen, ledningen och ansvaret för myndighetens sammantagna informationssäkerhetsarbete utvärderas och därefter fastställa ansvar och roller för informationssäkerhetsarbetet. Inom Polismyndigheten pågår en utredning och översyn om verksamhets- och säkerhetsskydd, som omfattar Polismyndighetens interna säkerhetsarbete.[1] Internrevisionen gör bedömningen att det tills resultatet av utredningen har medfört tydlighet i styrningen av informationssäkerheten bör det inrättas en interimistisk ansvarig för den myndighetsövergripande informationssäkerheten i enlighet med MSB: s föreskrifter.

Tabellen nedan visar att internrevisionens granskning har resulterat i totalt tre rekommendationer, fördelade utifrån internrevisionens modell för bedömning av brister som presenteras i rapporten.

		Antal
	Mycket väsentlig brist	1
	Väsentlig brist	2
	Mindre väsentlig brist	

[1] Uppdragsdirektiv om Polismyndighetens verksamhets- och säkerhetsskydd. Dnr A365.948/2018

2 Inledning

Granskningen har utförts i enlighet med revisionsplanen för 2016-2017.

Det öppna demokratiska samhället är beroende av säker hantering av information. Det innebär att både informationen i sig och de system som används för att förvara och överföra informationen behöver skyddas.[2] Informationssäkerhet rör hantering av, och säkerhet kring information. Detta gäller oavsett i vilken form informationen existerar och hanteras, om den är pappersbunden, digital information eller övriga uppgifter.

Enligt en rapport från Riksrevisionen om statliga myndigheters informationssäkerhetsarbete, är en vanligt förekommande iakttagelse att IT-säkerheten ofta är väl tillgodosedd, medan verksamheterna kan vara relativt omedvetna om deras ansvar för att säkra informationen i sig.[3]

Svenska myndigheter hanterar idag en mängd information med stor betydelse för en rad olika samhällsfunktioner. Information behöver kunna skyddas mot obehörig åtkomst (skydd av informationens konfidentialitet) men behöver även vara tillgänglig för behöriga när den ska användas (skydd för informationens tillgänglighet). Informationen behöver även skyddas mot obehöriga förändringar (skydd av informationens riktighet). För att säkerställa att dessa behov upprätthålls är det av grundläggande betydelse att det i efterhand går att spåra vem som har gjort vad i myndigheternas system (skydd av informationens spårbarhet). Säkerhet för information erhålls inte bara genom att införa olika säkerhetsåtgärder utan det är även av grundläggande vikt att på ett systematiskt sätt fortlöpande styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera, rapportera och förbättra säkerheten i myndighetens informationshantering. Det ger sammantaget möjlighet att upprätthålla en lämplig och tillräcklig nivå av säkerhet som är anpassad till bland annat verksamhetens behov, rättsliga krav samt identifierade hot och risker. Som stöd för ett sådant systematiskt arbete används ett ledningssystem för informationssäkerhet (LIS).[4] Ett ledningssystem är principer för att planera, leda, genomföra, utvärdera och förbättra en verksamhet på ett systematiskt sätt. Polismyndighetens information är en av de väsentligaste tillgångarna och ger myndigheten förutsättningar att utför sitt uppdrag på ett rättssäkert och effektivt sätt.

2.1 Bakgrund

Enligt MSB:s föreskrifter om statliga myndigheters informationssäkerhet ska varje myndighet bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Ledningssystemet ska utformas utifrån verksamhetens behov och vara styrande för all hantering av information som myndigheten ansvarar för.

[2] Regeringens skrivelse 2016/2017: 213. Nationell strategi för samhällets informations- och cybersäkerhet
[3] Riksrevisionen (2016: 8) Informationssäkerhetsarbete på nio myndigheter. En andra granskning av informationssäkerheten i staten.
[4] Konsekvensutredning rörande reviderade föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet MSB 2015-06-22

Det övergripande målet för Polismyndighetens it- och informationssäkerhetsarbete är att ha ett anpassat och ändamålsenligt skydd för myndighetens informationsbehandling. Ett anpassat och ändamålsenligt skydd innebär att säkerhetsåtgärder balanseras mot faktiska risker och kostnader.[5]

Enligt polisens arbetsordning (AO) och andra beslut är två funktioner processansvariga för informationssäkerheten. Dessa är it-avdelningen och verksamhetsskyddet på rikspolischefens kansli (RPCK). Enligt AO har it-avdelningen ansvar för it- och informationssäkerheten utom för fysiska dokument med text eller bild. Verksamhetsskyddet på RPCK har enligt ett beslut från 2016 ansvar för informationssäkerhet för text och bild och är tänkt att beskriva ansvaret utifrån AO.[6]

2.2 Syfte

Granskningen har utförts i enlighet med revisionsplan för 2016-2017.

Syftet med granskningen har varit att bedöma den interna styrningen och kontrollen av Polismyndighetens informationssäkerhetsarbete.

Granskningen har omfattat följande revisionsfrågor:

- Finns det en ändamålsenlig och tydlig ansvars- och befogenhetsfördelning för arbetet med informationssäkerhet?
- Finns det ändamålsenliga riktlinjer och andra styrdokument som reglerar ansvar och befogenheter för informationssäkerheten?
- Finns det en ändamålsenlig process/ledningssystem för informationssäkerhetsarbetet?

2.3 Omfattning och avgränsning

Granskningen har omfattat det myndighetsövergripande informationssäkerhetsarbetet. Granskningen, som inte enbart omfattar it- avdelningens arbete med informationssäkerhet, har genomförts på en övergripande nivå kring ledning och styrning av informationssäkerhetsarbetet. Det har inte att genomförts någon granskning av specifika IT-system. Efter att uppdragsbeskrivningen beslutades har internrevisionen gjort ytterligare en avgränsning avseende den del av informationssäkerheten som omfattar säkerhetsskyddet, även om det är en del av informationssäkerhetsarbetet. Skälet är att säkerhetsskyddsarbetet regleras av andra regelverk än MSB:s föreskrifter.

2.4 Metod och tillvägagångssätt

Granskningen har genomförts genom intervjuer med medarbetare från it- avdelningen och verksamhetsskyddet på RPCK, verksamhetsskydd vid två regionkanslier, NFC samt NOA. Analys av styrdokument och övriga beslut har också genomförts. Även en övergripande enkät har skickats informationsägarna.

[5] Polismyndighetens riktlinjer för behandling av information med stöd av It PM 2017:4
[6] A118.146/2016 ”Beslut för polisens säkerhets- och verksamhetsskydd”

Granskningen har utförts under perioden oktober 2017– april 2018, av internrevisorerna Marja Seppänen (ansvarig revisor) och Lars Agerberg.

Rapporten sakgranskades i maj 2018 av it-avdelningen, verksamhetsskyddet på rikspolischefens kansli (RPCK), NOA och de intervjuade regionerna. Begäran om inhämtande av åtgärdsförslag skickades till RPC kansli 2018-06-18. Svar med förslag på åtgärder med anledning av internrevisionens rekommendationer inkom till internrevisionen den 11/9 2018. Ytterligare handläggning av åtgärdsförslag genomfördes under oktober. Fullständiga åtgärdsförslag återges i bilaga till rapporten.

2.5 Bedömningsgrunder

Internrevisionens iakttagelser, bedömningar och grunder för lämnade rekommendationer framgår i rapportens avsnitt 3 och 4. Identifierade brister har bedömts vid tidpunkten för granskningen. Internrevisionens bedömning följer nedanstående mall.

Bedömning	Beskrivning
Röd - Mycket väsentlig brist	Brist som allvarligt påverkar Polismyndighetens måluppfyllelse enligt instruktion eller regleringsbrev och/eller medför stora negativa konsekvenser för Polismyndighetens verksamhet och/eller innebär att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet, redovisning och hushållning.
Orange - Väsentlig brist	Brist som påverkar den granskade verksamheten så att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.
Gul - Mindre väsentlig brist	Brist som inte påverkar den granskade verksamhetens måluppfyllelse men som medför negativa konsekvenser för verksamheten.

3 Ansvar och befogenheter inom informationssäkerhetsarbetet

3.1 Föreskrifter om statliga myndigheters informationssäkerhet

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet anger att varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS).[7] Myndigheten ska också upprätta en informationssäkerhetspolicy, och andra styrande dokument samt övrig dokumentation som krävs för att kunna bedriva ett ändamålsenligt informationssäkerhetsarbete. Av informationssäkerhetspolicyn ska ansvarsfördelningen för verksamhetens informationsmängder framgå. Vidare ska myndigheten även eftersträva en god säkerhetskultur för att alla i myndigheten ska ha kunskap och förståelse för behoven av säker hantering av information.
Ett ledningssystem för informationssäkerhet ska utformas utifrån verksamhetens behov och vara styrande för all hantering av information som myndigheten ansvarar för.

[7] MSBFS 2016:1

Genom ett LIS ska det tydliggöras hur myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete ser ut och tilldela nödvändiga befogenheter för de roller som arbetet med informationssäkerhet kräver. Detta gäller särskilt för den eller de som ska utses för att leda och samordna arbetet.[8]

I MSB:s uppdaterade metodstöd betonas att det är av stor vikt att den som har ansvaret för informationssäkerhetsarbetet har ett stöd från ledningen och att ledningen kommunicerar ut mandatet för rollen och vikten av ett bra informationssäkerhetsarbete i organisationen.[9]

3.1.1 Ansvar och befogenheter inom Polismyndigheten

Iakttagelser
Polismyndighetens informationssäkerhetsarbete är en del av myndighetens verksamhetsskydd som består av fyra målområden: skydd av medarbetare, skydd av information (informationssäkerhet), skydd av egendom (tillträdesbegränsningar) och anställning och uppdrag (säkerhetsprövning).[10]

Internrevisionen noterar att arbetet med att upprätthålla informationssäkerheten är fördelat på flera roller på olika nivåer i verksamheten.

Utgångspunkten för Polismyndigheten är att ansvaret för själva informationssäkerhetsarbetet följer det ordinarie verksamhetsansvaret.[11] I AO och i andra beslut framgår att processansvaret för den del av verksamhetsskyddet som omfattar informationssäkerhet är fördelat på två funktioner, it- avdelningen och verksamhetsskyddet. It- avdelningens ansvar framgår av 3 kap 21 §. Avdelningen har verksamhetsansvar för och chefen för avdelningen är tillika processägare för den del av verksamhets- och säkerhetsskyddet som omfattar it- och informationssäkerhet, utom för fysiska dokument med text eller bild. Verksamhetsskyddet på RPCK har ett ansvar för verksamhets- och säkerhetsskydd som omfattar text och bild.[12] Utöver det framgår i AO att it- avdelningen ska ha verksamhetsansvar för den del av verksamhets- och säkerhetsskyddet som omfattar it- och informationssäkerhet, utom för fysiska dokument med text eller bild, för avdelningarna och regionerna Mitt och Öst.

Vidare i AO, avsnittet 3 kap 3 § beskrivs processer: Verksamhetsskyddschefen på RPCK är processägare för säkerhetsskyddet, förutom den del av säkerhetsskyddet som omfattar it- och informationssäkerhet. Regionkanslierna har också ansvar för informationssäkerhet enligt 3 kap 15 §. Regionkansliet ska ha verksamhetsansvar för verksamhets- och säkerhetsskyddet inklusive informationssäkerhet och signalskydd inom regionen och de regionalt placerade avdelningarna.

[8] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1)
9 https://www.informationssakerhet.se/om-webbplatsen/malgrupper/sakerhetsansvarig/ 180410
[10] Beslut A118.146/2016. ”Beslut för polisens säkerhets- och verksamhetsskydd”
[11] Polismyndighetens riktlinjer för behandling av information med stöd av It PM 2017:4
[12] Se ovan beslut i not 8.

För verksamhetsskyddet finns en policy, som omfattar skydd av medarbetare, information och egendom.[13] I verksamhetsskyddspolicyn noterar internrevisionen att det inte finns en uppdelning av informationssäkerhetsansvaret i IT-system och text och bild och övrigt så som görs i AO. Internrevisionen noterar också att det saknas myndighetsinterna riktlinjer för skyddet av information avseende text eller bild. Av ett beslut fattat 2016 noterar internrevisionen att verksamhetsskyddet på RPCK utifrån sitt processansvar för verksamhets- och säkerhetsskydd ska ta fram riktlinjer för målområdet text och bild.[14]

I Polismyndighetens ”Riktlinjer för säkerhet vid behandling av information med stöd av it”, PM 2017: 4 anges att två roller är av särskild vikt för en god och ändamålsenlig it- och informationssäkerhet, dessa är informationsägare och produktägare. Av AO 3 kap 16 § framgår det att avdelningarna är informationsägare: ”Vidare ska avdelningarna vara informationsägare och kravställare av it- system inom avdelningens ansvarsområde”. Polismyndighetens informationsägare är ansvariga för den information som behandlas i ett it- system och för att information hanteras i enlighet med gällande författningar och Polismyndighetens styrdokument”. I 3 kap 21 § i AO anges att it- avdelningen ska bistå avdelningarna så att dessa kan fullgöra sitt ansvar som kravställare av it- system.
Av den övergripande enkäten som internrevisionen skickade till informationsägarna, (som i de flesta fall är processägare eller delegerar processägarskapet) framgår att avdelningarna och deras processägare har löpande kontakter med it- avdelningens produktägare som ansvarar för att ta fram säkerhetslösningar för informationsägarna. Arbetet sker genom en samarbetsmodell. I informationsägarnas ansvar ingår bland annat att ta initiativ för att informationsskyddsklassa sin information. Internrevisionen har informerats om att ett arbete med att ta fram en handbok för informationsskyddsklassning har initierats av it-avdelningen.

Internrevisionen noterar att det i riktlinjer PM 2017:4 framgår att: ”En tydlig organisation och ansvarsfördelning för säkerhetsarbetet är en avgörande förutsättning för att myndigheten ska kunna leva upp till fastställda säkerhetskrav”.[15] I riktlinjen finns även en avgränsning att den omfattar all informationsbehandling med stöd av it, det vill säga den del av Polismyndighetens verksamhetsskydd som omfattar it- och informationssäkerhet, utom för text och bild.

Inom myndigheten finns också att antal riktlinjer för mobilitet, sociala medier m.m. Det finns också en övergripande broschyr framtagen av it- avdelningen för polisens anställda, ”Polisens säkerhetsinformation” och även en riktlinje för Polismyndighetens signalskyddstjänst (PM 2018:19).

Bedömning

Internrevisionen bedömer att myndighetens informationssäkerhetsarbete styrs, leds och organiseras på ett traditionellt sätt, sett ur ett övergripande säkerhetsperspektiv, där säkerhetsskydd och annan fysisk säkerhet utgör en del och där informationssäkerhet och IT-säkerhet utgör den andra delen.[16] Internrevisionen konstaterar att den tydliga organi-

[13] Polismyndighetens verksamhetsskydds policy, PM 2015:21
[14] Beslut A118.146/2016. ”Beslut för polisens säkerhets- och verksamhetsskydd” som anger att ett av fyra målområden inom verksamhetsskyddet är informationssäkerhet.
[15] Polismyndighetens riktlinjer för behandling av information med stöd av It 2017:4
[16] Svenska kraftnät (2014) ”Vägledning informations- och IT-säkerhet samt säkerhetsskydd”

sations- och ansvarsfördelningen för säkerhetsarbetet i myndigheten som it- avdelning beskriver i sina riktlinjer, saknas.

Internrevisionen noterar att det saknas styrdokument för det myndighetsövergripande informationssäkerhetsarbetet i samlad form, såsom framgår av MSB:s föreskrifter. Internrevisionen anser att it- avdelningens riktlinjer har tonvikt på IT-säkerhet då den omfattar informationsbehandling med stöd av it samt att det för verksamhetsskyddets informationssäkerhetsansvar saknas styrdokument. Vidare noterar internrevisionen att den policy som finns för verksamhetsskyddet inte överensstämmer med AO:s reglering av processansvar för informationssäkerhetsarbetet.

Internrevisionen bedömer att informationsägarnas ansvar utgör en stor del i informationssäkerhetsarbetet. Internrevisionen har dock inte funnit styrdokument /riktlinjer/handbok på en myndighetsövergripande nivå för hur informationsägarna praktiskt ska agera för att kunna sitt ansvar inom informationssäkerhetarbetet. Den kommande handboken för informationsklassning borde därför utgöra del av ett sådant stöd.

Var ansvaret för det samlade informationssäkerhetsarbetet finns är inte uttalat i de interna styrdokument som finns, AO, it- avdelningens riktlinjer och inriktningsbeslut för verksamhetsskyddet. Internrevisionen bedömer att det övergripande ansvaret för att leda och samordna arbetet med informationssäkerhet i myndigheten är ovanlig genom den nuvarande uppdelningen av processansvaret och vilket kan försvåra införandet av ett för polisen anpassat LIS. Internrevisionen bedömer att det kan uppstå stuprörsproblematik som inverkar negativt på effektiviteten och kvalitén i informationssäkerhetsarbetet. Internrevisionen bedömer att detta kan medföra missförstånd, sårbarheter och merarbete. Det för också med sig risker/svårigheter att rapportera det övergripande säkerhetsläget till myndighetens ledning. Ledning, samordning och uppföljning av informationssäkerhetsarbetet är till stora delar ett strategiskt arbete som behöver planeras, ledas och styras. I det ingår att upprätthålla en kontinuitetsförmåga för att uppnå riktighet, konifidentialitet och tillgänglighet till informationen.[17] Internrevisionens bedömer ett strategiskt arbete med informationssäkerhet behövs för att kunna skapa ett systematiskt informationssäkerhetsarbete som är anpassat till myndighetens behov och som kan fungera över längre tid. Internrevisionens bedömning är att detta i dagsläget saknas, alternativt inte är prioriterat.

Internrevisionen har tagit del av information om att en översyn av Polismyndighetens verksamhets- och säkerhetsskyddsarbete ska genomföras av en särskild utredare.[18] Tills översynen är klar och eventuella förändringar genomförs för verksamhet- och säkerhetsskydd gör internrevisionen bedömningen att en interimistisk ansvarig för Polismyndighetens informationssäkerhet utses i enlighet med MSB: s föreskrifter.

[17] Kontinuitetsförmågan är särskilt viktig utifrån polisens samhällsviktiga verksamhet så som MSB definerar det, inom samhällssektorn ”Skydd och säkerhet”. Syftet är att ha en god förmåga att motstå och hantera störningar så att de negativa effekterna på samhället blir så små som möjligt.
[18] Uppdragsdirektiv om Polismyndighetens verksamhets- och säkerhetsskydd. Dnr A365.948/2018

Rekommendation 3.1.1 - 1

Röd – Mycket väsentlig brist

Internrevisionen rekommenderar att översynen inkluderar att utse ansvar, roller, befogenheter och organisation för Polismyndighetens samlade informationssäkerhetsarbete i enlighet med MSB: s föreskrifter.

Konsekvenserna av om rekommendationen inte följs är att det kan medföra stora negativa konsekvenser för Polismyndighetens verksamhet och att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet och hushållning med statens medel. Bristande informationssäkerhetsarbete kan medföra att verksamheten inte kan bedrivas på ett ändamålsenligt och effektivt sätt, otillräckligt skydd av den personliga integriteten samt störningar i samhällsviktig verksamhet. Allmänhetens förtroende för polisen kan skadas.

Rekommendation 3.1.1 - 2

B. Orange – Väsentlig brist

Internrevisionen rekommenderar att it-avdelningen och verksamhetsskyddet på RPCK gemensamt tar fram styrdokument/riktlinjer som reglerar myndighetens sammantagna informationssäkerhetsarbete.

Konsekvenserna av om rekommendationen inte följs är att det kan medföra betydande negativa konsekvenser för Polismyndighetens verksamhet och att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet, redovisning och hushållning. Bristande informationssäkerhetsarbete kan medföra att verksamheten inte kan bedrivas på ett ändamålsenligt och effektivt sätt, otillräckligt skydd av den person liga integriteten samt störningar i samhällsviktig verksamhet.

4 Process/ledningssystem för informationssäkerhetsarbetet

4.1 Styrning av informationssäkerhet

Enlig MSB:s föreskrifter har myndighetens ledning ansvar för att styra och skapa förutsättningar för myndighetens informationssäkerhetsarbete. Det förutsätter uppdaterad kunskap om organisationens behov av och förutsättningar för säker hantering av information. Myndighetens ledning bör enligt MSB:s föreskrifters allmänna råd följa upp och utvärdera informationssäkerhetsarbetet flera gånger per år.

Genom ett ledningssystem tydliggör och säkerställer myndighetsledningen att informationssäkerhetsarbetet bedrivs samordnat samt att det regelbundet utvärderas och löpande utvecklas. Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet och regelbunden information ska lämnas till myndighetsledningen. Ett effektivt och välorganiserat

it- och informationssäkerhetsarbete är en förutsättning för att kunna utföra Polismyndighetens uppgifter.

4.1.1 Styrning av informationssäkerhet inom Polismyndigheten

Internrevisionen konstaterar att det i dagsläget inte finns ett ledningssystem för informationssäkerhet och ingen övergripande process eller utsedd ansvarig för myndighetens samlade informationssäkerhetsarbete. MSB:s krav på styrning, samordning och ledning av informationssäkerheten inom myndigheten omhändertas inte utifrån hur ansvaret för informationssäkerhet nu är fördelat mellan verksamhetsskyddet och it-avdelningen.

Internrevisionen konstaterar också att företräde har getts till arbetet med att öka och säkerställa it- leveranser.[19] Resurser har då gått till it-leveranser, att ta fram och införa ett LIS har fått stå tillbaka. Enligt it- avdelningen är ambitionen att Polismyndigheten ska ha ett ledningssystem för it- och informationssäkerhet som beskriver hur verksamhetens säkerhetsarbete inom området ska styras och utföras. Delar av ett ledningssystem finns men det behöver utvecklas ytterligare för att få till mer av ett myndighetsövergripande ledningssystem. Ledningssystemet ska också enligt it-avdelningens ambition vara uppbyggt enligt praxis så att arbetet ska kunna utföras på ett systematiskt sätt och med ständiga förbättringar.[20]

Informationssäkerhetsarbete förutsätter även en adekvat resurstilldelning. Under 2016 genomförde it- avdelningen en kompetens – och dimensioneringsanalys av regionernas behov av resurser för att utföra det operativa informationssäkerhetsarbetet.[21] Målet för 2016-2017 beskrevs vara att säkerställa att varje region har 1-2 resurser. Målet för 2020 beskrivs vara att rekrytera ytterligare 1-2 personer beroende på region men då med personer med särskild kompetens inom informationssäkerhetsområdet. It- avdelningen har för avsikt att göra en uppdatering av dimensioneringsanalysen under 2018.[22]

Efter ett beslut taget 2016-03-18 av rikspolischefen ska informationssäkerhetsamordnarna på regionerna ingå i verksamhetsskyddsfunktionerna på regionkanslierna och inte som tidigare höra till it- avdelningen[23]. It- avdelningen ser samordnarna som sin förlängda arm i informationssäkerhetsarbetet då de utför det operativa informationssäkerhetsarbetet. Internrevisionen noterar att informationssäkerhetsamordnarna dock praktiskt arbetsleds av regionkanslierna. De medarbetare som arbetar specifikt med informationssäkerhet är en viktig stödfunktion i myndigheten. Dessa medarbetare ska ansvara för att själva arbetet med informationssäkerhet fungerar på ett tillräckligt bra sätt. De ska däremot inte ha ett formellt ansvar för informationssäkerheten, utan det huvudsakliga syftet med deras roll och arbete är i stället att stötta ledningen, cheferna och medarbetarna. Det innebär att se till så att ledning, chefer och medarbetare tar ansvar för informationssäkerheten i sin verksamhet. Ofta består arbetet av att utbilda och informera om informationssäkerhet för de anställda och ge chefer råd och stöd kring informationssäkerhet samt följa upp och kontrollera regelefterlevnad. Dessa arbetsuppgifter genom-

[19] Information som erhölls vid möte med it -avdelningen 20 oktober 2017, bild nr 49 i ppt
[20] Med praxis avses att arbeta efter internationella standards så som t ex ISO 27001 och ISO 27002
[21] Kompetens- och dimensioneringsanalys informationssäkerhet 2016-07-13
[22] Polismyndighetens analys och bedömning av informationssäkerheten i den egna verksamheten. Redovisning av regeringsuppdrag. Dnr A308.466/2017.
[23] It-021/2016 sak nr 129.

förs på olika sätt och i olika omfattning i varje region. Internrevisionen noterar att det saknas enhetliga rutiner, riktlinjer och planer för vad som ska utföras av medarbetarna som arbetar med informationssäkerhet på regionerna så att det bedrivs systematiskt och efter enhetliga säkerhetskrav. Det har dock tagits initiativ till att ta fram planer. Internrevisionen noterar också att alla regioner inte har tillsatt en informationssäkerhetssamordnare.

Internrevisionen noterar att genom att placera informationssäkerhetsamordnarna på regionskansliernas verksamhetsskydd har det regionala informationssäkerhetsarbetet kommit att omfatta all informationssäkerhet och är inte uppdelat i två processer och två organisatoriska enheter så som på nationell nivå.

Bedömning

Internrevisionen bedömer att det övergripande ansvaret för att leda och samordna arbetet med informationssäkerhet i myndigheten är otydligt. Var ansvaret för arbetet som helhet framgår inte av de interna styrdokument som finns, AO och it-avdelningens riktlinjer. Ledning, samordning och uppföljning av informationssäkerhetsarbetet är till stora delar strategiskt arbete som behöver planeras. Internrevisionens bedömer att det strategiska perspektivet behövs för att kunna skapa ett systematiskt arbete som är anpassat till myndigheten och kan fungera över längre tid, men att det i dagsläget saknas, alternativt inte är prioriterat.

Internrevisionen bedömer att det inte finns tillräckliga resurser tillsatta på regionerna för att myndighetens informationssäkerhetsarbete kan genomföras systematiskt genom ett LIS och i tillräcklig och nödvändig omfattning. De informationssäkerhetssamordnare som finns vid regionerna har skiftande kompetens varför it- avdelningens behov en förlängd arm inte tillgodoses. Interrevisionen bedömer att det finns behov av informationssäkerhetskompetens och resurser på regionerna för att linjeverksamheten praktiskt ska kunna ta sitt ansvar för informationssäkerheten. De informationssäkerhetsresurserna som idag finns på regionerna har varken it- avdelningen eller verksamhetsskyddet på RPCK mandat att styra, då de arbetsleds av regionernas kanslier. Att det saknas resurser för att bedriva systematiskt informationssäkerhetsarbete bedömer internrevisionen ger uttryck för att risker för polisens informationstillgångar är underskattade.

Internrevisionen anser att it- och informationssäkerhet utgör en del i myndighetens övergripande arbete med intern styrning och kontroll (ISK) och ska ses som en integrerad del i processen för ISK

Vidare bedömer internrevisionen att it- avdelningens behov av att utveckla och ta fram it- stöd för kärnverksamheten, har fört med sig en viss nedprioritering av att ta fram, införa och använda ett LIS vilket innebär ett val med en viss grad av riskaptit. Ledningen behöver även ur detta perspektiv löpande informeras om informationssäkerhetsläget eftersom de är ytterst ansvariga.

För att främja en god säkerhetskultur bedömer internrevisionen att det finns ett behov av att i högre grad rapportera risker och status för informationssäkerheten till Polismyndighetens ledning.

Rekommendation 4.1.1

Orange – Väsentlig brist

Internrevisionen rekommenderar att it-avdelningen och verksamhetsskyddet på RPCK i samverkan:

- prioriterar arbetet med att ta fram och införa ett för Polismyndigheten anpassat LIS.
- gör en bedömning av vilka resurser som behövs för att ta fram ett för Polismyndigheten anpassat LIS
- definierar arbetsuppgifter och ansvar för informationssäkerhetsamordnarna på regionerna i syfte att säkerställa ett systematiskt informationssäkerhetsarbete.

Konsekvenserna av om rekommendationen inte följs är att det kan medföra betydande negativa konsekvenser för Polismyndighetens verksamhet och att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet, redovisning och hushållning Bristande informationssäkerhetsarbete kan medföra att verksamheten inte kan bedrivas på ett ändamålsenligt och effektivt sätt, otillräckligt skydd av den personliga integriteten samt störningar i samhällsviktig verksamhet.

5 Sammanfattande bedömning av revisionsfrågorna

Internrevisionen bedömer att det finns brister i den interna styrningen och kontrollen av informationssäkerhetsarbetet inom myndigheten. Intern styrning och kontroll av informations konfidentialitet, riktighet, tillgänglighet och spårbarhet behöver ske genom processen LIS, ledningssystem för informationssäkerhet. Internrevisionen bedömer därför att informationssäkerheten inom Polismyndigheten omfattar mer än it-avdelningens uppdrag. Internrevisionen bedömer att för att de ska finnas förutsättningar för att upprätta och använda ett LIS som del av ISK så behöver styrningen, ledningen och ansvaret för myndighetens sammantagna informationssäkerhetsarbete utvärderas och därefter fastställa ansvar och roller för informationssäkerhetsarbetet.

Internrevisionen bedömer att Polismyndighetens nuvarande uppdelning i ansvaret för informationssäkerhetsarbetet mellan informationsbehandling med stöd av it, och informationsbehandling/hantering av fysiska dokument kan komma att försvåra ambitionen att ta fram och arbeta genom ett för polisens anpassat LIS. Det kan även leda till att ansvar för vissa kategorier av informationstillgångar kommer att falla mellan stolar. Internrevisionen menar att arbetet för utformning av ett LIS för polisen är beroende av att det finns ett övergripande ansvar för hela informationssäkerhetsområdet.

Internrevisionen noterar att det saknas styrdokument då det myndighetsövergripande informationssäkerhetsarbetet inte bedrivs i samlad form (såsom framgår av MSB:s föreskrifter). Internrevisionen bedömer också att de riktlinjer och eventuella andra styrdokument som finns inte är tillräckligt ändamålsenliga i syfte att i ett samlat grepp reglera informationssäkerhetsarbetet för att stödja verksamheten.

Internrevisionens bedömning är att myndigheten inte har en ändamålsenlig process för styrning av informationssäkerhetsarbetet. Dels är processansvaret för informationssäkerhet delad mellan två funktioner, dels har styrningen av informationssäkerheten fördelats efter lagringsmedia/form och inte efter skyddsvärde och mål för myndighetens informationssäkerhet. Utgångspunkten för ett myndighetsövergripande informationssäkerhetsarbetet är att se till att hela organisationen kan ta ett gemensamt ansvar för informationssäkerheten så som det framgår av lagar, interna riktlinjer och andra styrdokument.

Internrevisionen bedömer att det inte finns tillräcklig kompetens och resurser tillsatta på regionerna för att myndighetens informationssäkerhetsarbete kan genomföras systematiskt och i tillräcklig och nödvändig omfattning. Den dimensionering som finns på regionerna i dag ger inte förutsättningar att arbeta med ett systematiskt informationssäkerhetsarbete. Att det saknas resurser för att bedriva informationssäkerhetsarbete kan enligt internrevisionen bero på att riskerna för polisens informationstillgångar har underskattats.

Ett stort förberedande arbete har dock gjorts av it-avdelningen som har resulterat i en riktlinje för säkerhet avseende informationsbehandling med stöd av it.
En viktig förutsättning för att lägga grunden till en god informationssäkerhetskultur och för att skapa förståelse för informationssäkerhet är också att myndighetens ledning visar på behovet av en god övergripande säkerhetskultur.

Marja Seppänen

Lars Agerberg

Datum	Beslutsnummer
2018-12-10	RPC 156/18
Diarienr, ärende	Saknr
A512.866/2017	977

Beslutande	Föredragande
Rikspolischefen Anders Thornberg	Polisintendenten Stefan Eurenius

Övriga som deltagit i den slutliga handläggningen
Avdelningschefen Martin Valfridsson MV
Internrevisionschefen Stina N Kristiansson SK
Avdelningschefen Eva Årestad Radner EÅR
Avdelningschefen Tomas Landeström TL

Beslut om åtgärder med anledning av internrevisionens granskning av Polismyndighetens informationssäkerhetsarbete.

Beslut

Bakgrund

Internrevisionen har genomfört en granskning av Polismyndighetens informationssäkerhetsarbete. Granskningen har resulterat i ett antal iakttagelser och rekommendationer.

It-avdelningen och verksamhetsskyddsenheten vid rikspolischefens kansli har lämnat förslag till åtgärder med anledning av rekommendationerna. Delar av internrevisionens rekommendationer kommer vidare att omhändertas inom ramen för utredningen om Polismyndighetens verksamhets- och säkerhetsskydd (dnr A365.948/2018). Det gäller bl.a. hur informationssäkerhetsarbetet inom myndigheten bör organiseras.

Beslut

Polismyndigheten beslutar avseende

Rekommendation 3.1.1 -1 och 2 att

Utredningen om Polismyndighetens verksamhets- och säkerhetsskydd redovisar sina förslag den 31 december 2018. Rekommendationerna kommer att tas om hand i samband med omhändertagande av utredarens förslag

Rekommendation 4.1.1 att

a. It-avdelningen och verksamhetsskyddsenheten vid Rikspolischefens kansli tillsammans ska ta fram och införa ett gemensamt ledningssystem för informationssäkerhet (LIS) som omfattar myndighetens hela informationssäkerhetsområde. Arbetet ska påbörjas under 2018 och slutföras efter det att utredningen om Polismyndighetens verksamhets- och säkerhetsskydd är genomförd.
b. It-avdelningen och verksamhetsskyddsenheten vid Rikspolischefens kansli ska säkerställa att de har rätt kompetens inom informationssäkerhetsområdet.

Chefen för it-avdelningen och chefen för rikspolischefens kansli ansvarar för åtgärdernas genomförande. Åtgärderna ska vara genomförda senast den 31 december 2019.

Kostnad	Finansiering
Inom budget	

Vid protokollet

Stefan Eurenius

Justeras

Anders Thornberg

Sändlista	Kopia till
Samtliga avdelningar och regioner	Arbetstagarorganisationerna