Granskning av polisens förmåga att förebygga, upptäcka och hantera oegentligheter i polisens it-system

Internrevisionen

2019-04-01

Granskning av polisens förmåga att förebygga, upptäcka och hantera oegentligheter i polisens it-system

INNEHÅLL

1 Sammanfattning

Internrevisionen har konstaterat brister i den kontroll som syftar till att förebygga och upptäcka oegentligheter i polisens it-system. När det gäller att hantera sådana oegentligheter är förmågan bättre genom den lagstiftning och struktur som finns och som tillämpas av SU, PAN och GSD.

Internrevisionens bedömning är att ekonomiavdelningen (EA) bör utveckla myndighetens riktlinje för intern styrning och kontroll (ISK) så att den även omfattar arbetet mot oegentlighetsrisker inom myndighetens ISK process i enlighet med ESV: s riktlinjer.

It-avdelningen bör, med utgångspunkt från riktlinje PM 2017:4 och EA:s riktlinje för Polismyndighetens övergripande ISK-arbete, ta fram en rutin för att på ett systematiskt sätt öka polisens förmåga att förebygga och upptäcka oegentligheter i polisens it-system. Detta i syfte att stödja informationsägarna att bli mer aktiva i sitt informationsägaransvar så som det framgår av Polismyndighetens arbetsordning (AO).

Det finns olika funktioner som hanterar uppdagade oegentligheter i polisens it-system. Dock saknas det ett myndighetsövergripande tydligt, direkt och uttalat ansvarsutpekande för hur oegentligheter i it- systemen ska förebyggas och upptäckas. Internrevisonen anser därför att det är angeläget att de olika funktionerna i samråd tar fram styrdokument för ökad enhetlighet på området och att detta ska framgå av AO. Internrevisionen rekommenderar att de ovan utpekade funktionerna etablerar en strukturerad samverkan för att gemensamt skapa ökade förutsättningar för ett systematiskt arbete mot oegentligheter i polisens it-system med utgångspunkt från myndighetens arbete med intern styrning och kontroll.

Internrevisionen rekommenderar därför att myndighetsledningen inom ramen för befintlig organisation tydliggör styrningen, ansvarsfördelningen och processen i arbetet med att upptäcka, hantera och förebygga oegentligheter i polisens it-system.

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

		Antal
	Mycket väsentlig brist	2
	Väsentlig brist	6
	Mindre väsentlig brist	

2 Inledning

Granskningen utförs i enlighet med revisionsplan för 2016-17.

2.1 Bakgrund

Ekonomistyrningsverket använder begreppet oegentligheter som ett samlingsbegrepp för oönskade beteenden/handlingssätt med konsekvenser för myndighetens anseende och/eller verksamhet. Begreppet oegentligheter omfattar även korruption. För en myndighet är det av central betydelse hur sådana händelser hanteras.[1]

2.2 Syfte och mål

Syftet med granskningen är att bedöma den interna styrningen och kontrollen av processen för att hantera oegentligheter inom myndigheten med fokus på hur polisanställda, hanterar polisens information i it- system och hur oegentligheter upptäcks, hanteras och förebyggs.

Målet med granskningen är att säkerställa att 3 § i myndighetsförordningen efterlevs vad gäller att verksamheten bedrivs enligt gällande rätt.

2.3 Omfattning och avgränsning

Granskningen omfattar följande revisionsfrågor:

- Finns det ändamålsenliga riktlinjer och andra styrdokument som reglerar ansvaret och hanteringen av oegentligheter?
- Finns det en ändmålsenlig och tydlig ansvars- och befogenhetsfördelning?
- Finns det en ändamålsenlig process för att upptäcka, hantera och förebygga oegentligheter?

Granskning avgränsas till verksamhetens (informationsägarna m.fl.) aktiviteter för att upptäcka, hantera och förebygga oegentligheter och otillåtna aktiviteter i polisens it-system. Av särskilt intresse är hur centrala säkerhetsloggen, CSL[2], används för att upptäcka interna oegentligheter som riktas mot Allmänna spaningsregistret (Asp), Datoriserad utredningsrutin med tvångsmedel (Durtvå), Rationell anmälans rutin (Rar) samt Centralt operativt planeringssystem (Cops). Granskningen omfattar inte SU:s brottsutredande verksamhet.

2.4 Metod och tillvägagångssätt

Granskningen har genomförts under första halvåret 2017 av ansvarig revisor Philip Jansson och medverkande revisorer Marja Seppänen och Winfred Nionzima.

[1] ESV 2016:24, Vägledning. Oegentligheter och intern styrning och kontroll.
[2] PM utgiven av IT-säkerhet/Loggning och Behörighet, daterat 2017-10-16: CSL är Polismyndighetens centrala funktion för insamling, lagring och analys av loggar som visar vad användare gjort i polisens it-system. CSL:s huvudsyften är att; skydda den enskildes integritet, minska risken för att sekretessbelagd eller skyddsvärd information röjs, ta fram bevismaterial av god kvalitet ur säkerhetsloggar för utredning av eventuella incidenter, samt ge möjlighet till larm i realtid vid misstänkta situationer (se intrapolis).

I granskningen har olika dokument granskats och intervjuer genomförts med informationsägarna för de under avsnitt 2.3 uppräknade systemen, polisens personuppgiftsombud och representanter för it-säkerhetsenheten (it-säk) samt verksamhetsskyddet nationellt och regionalt.

Internrevisionen har också begärt in kopior av beställningar av loggutdrag från it-säk av uppgifter från CSL, för perioden 160401 till 170331. Syftet med genomgången har varit att få fram en översiktlig bild över i vilken utsträckning informationsägarna är aktiva för att kontrollera vad användarna gör i deras respektive system. Kopiorna avsåg samtliga beställningar med undantag för beställningar från avdelningen för särskilda utredningar (SU) vilka görs i ett brottsutredande syfte.

Rapporten sakgranskades under perioden januari-februari 2018 av it-, ekonomi-, rätts-, HR- och nationella operativa avdelningen samt rikspolischefens kansli och avdelningen för särskilda utredningar. I avvaktan på beslut avstannade arbetet med rapporten under perioden mars till juni 2018. Begäran om inhämtande av åtgärdsförslag skickades till Rikspolischefens kansli (RPCK) den 21 juni 2018. Svar med förslag på åtgärder med anledning av internrevisionens rekommendationer har lämnats av verksamhetsansvariga. RPC har den 26 mars 2019 fattat beslut om åtgärder utifrån internrevisionens lämnade rekommendationer.

2.5 Bedömningsgrunder

Internrevisionens iakttagelser, bedömningar och grunder för lämnade rekommendationer framgår av den löpande texten i rapporten. För respektive rekommendation har internrevisionen bedömt bristen 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 Allmänt om oegentligheter

Riksrevisionen konstaterar i rapporten Statliga myndigheters skydd mot korruption[3] att det förekommer kända risker för korruption när det t.ex. gäller områden som avser brottsutredningar och hantering av känslig information. ESV definierar begreppet oe-

[3] RiR 2013:2.

gentligheter som ett samlingsbegrepp för hela gruppen av oönskade beteenden/handlingssätt med konsekvenser för myndighetens anseende och/eller verksamhet där olika former av korruption ingår.[4]

Enligt Brottsförebyggande rådet[5], Brå, är den vanligaste formen av oegentligheter att medarbetare/insider tar fram och lämnar ut känslig – i många fall sekretessbelagd – information. Det kan vara kunskap om myndighetens arbetsformer, bemanning, och placering av värdefullt material eller upplysningar om brister i myndighetens kontroll- och säkerhetssystem. Olika verksamheter har olika oegentlighetsrisker. En grundläggande del i arbetet med att förebygga risker för oegentligheter är att myndigheten skaffar sig en bild av vilka de interna riskerna är och inom vilka områden de finns. I stort sett alla myndigheter har ett stort it-beroende. Det behövs både ett skydd mot externt intrång, ett väl fungerande internt behörighetssystem och ett fungerande skydd i form av backup av informationen.[6]

Medarbetare, dvs. anställda och uppdragstagare (t.ex. konsulter, annan inhyrd personal) samt tjänstemän från andra myndigheter som har tillgång till polisens it-system, har ett ansvar att följa gällande regelverk inom it- och informationssäkerhetsområdet, såsom lagar, förordningar och föreskrifter. Avsteg från regelverket kan leda till att den enskilde kan dömas för dataintrång men kan också innebära disciplinära åtgärder från polisens personalansvarsnämnd (Pan). De ska även vara uppmärksamma på och rapportera säkerhetsbrister, säkerhetsincidenter och avvikelser som kan påverka myndighetens säkerhet till närmaste chef eller via myndighetens beslutade rutiner för incidentrapportering.[7]

Ansvaret för it- och informationssäkerhet inom Polismyndigheten följer det ordinarie linje- och verksamhetsansvaret som en del av Polismyndighetens ISK-arbete. Det innebär att chefer inom sina verksamhetsområden, med stöd av fastställda riktlinjer och tillhörande handböcker m.m., ska arbeta förebyggande och systematiskt med informations- och it-säkerhet i den egna verksamheten samt följa upp att säkerheten följs för att upprätthålla en anpassad säkerhetsnivå. Risker som är förknippade med verksamhetens informations- och it-säkerhet ska identifieras och hanteras.[8]

4 Intern styrning och kontroll

Iakttagelse

Intern styrning och kontroll är en förutsättning för att myndighetsledningen ska kunna fullgöra kraven på verksamheten enligt myndighetsförordningen. I ansvaret ingår att vidta de åtgärder som är nödvändiga för att hantera risker för oegentligheter.[9] Enligt Polismyndighetens arbetsordning (AO) 3 kap. 19 § punkt fyra är chefen för ekonomiav-

[4] ESV 2016:24, sidan 8.
[5] Brå:s rapport 2014: 4 Korruption i myndighetssverige. Otillåten påverkan mot insider.
[6] ESV 2016:24, sidan 17.
[7] Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it. PM 2017:4. Saknr 174.
[8] Se föregående not samt Polismyndighetens AO 5 kap. 8 §.
[9] ESV (2016: 24) Vägledning Oegentligheter och intern styrning och kontroll. Att komma vidare i arbetet med att förebygga och upptäcka oegentligheter.

delningen processägare för att säkerställa en väl fungerande process för intern styrning och kontroll.

Polismyndighetens riktlinjer för intern styrning och kontroll[10] är ett övergripande styrdokument för arbetet med ISK i Polismyndigheten med utgångspunkt från förordning (2007:603) om intern styrning och kontroll (FISK). Syftet med riktlinjerna är att styra arbetet kring intern styrning och kontroll som en del av verksamhetsstyrningen samt att ge stöd till dem som ansvarar för och arbetar med genomförandet av den interna styrningen och kontrollen i verksamheten.

När det gäller Polismyndighetens arbete mot oegentligheter framgår det av riktlinjerna (avsnitt 4, sidan 9) att ”Polismyndigheten är en komplex verksamhet med många olika verksamhetsområden och det är därför inte möjligt att ta fram generella åtgärder mot oegentligheter, som kan anses vara tillräckliga och ändamålsenliga för de flesta situationer då verksamheten är så diversifierad”. Åtgärder för att förebygga och upptäcka oegentligheter beskrivs av ekonomiavdelningen, EA, som ”situationsberoende, där ansvarig chef behöver ta ställning till effektiviteten i den interna kontrollen för det särskilda verksamhetsområdet”. Varje chef har enligt Polismyndighetens AO 5 kap. 8 § ett ansvar för att den interna styrningen och kontrollen är betryggande.

EA har enligt Polismyndighetens AO ett processansvar för att säkerställa en väl fungerande process för intern styrning och kontroll och samordnar Polismyndighetens rapportering av den interna styrningen och kontrollen. I anvisningar till regioner och avdelningar inför myndighetens tertialuppföljningar av risker anges inte att det ska ske en bedömning av om det finns risker för olika typer av oegentligheter.[11]

It-avdelningen är enligt Polismyndighetens AO 3 kap. 21 § punkt 10 och riktlinje PM 2017:4, bl.a. processägare för den del av verksamhets- och säkerhetsskyddet som omfattar it- och informationssäkerhet, utom för fysiska dokument med text eller bild, och ska stödja avdelningarna med it- och informationssäkerhet.

Av Polismyndighetens AO följer enligt 3 kap. 16 § att de nationella avdelningarna är informationsägare och kravställare av it-system inom avdelningens ansvarsområde. De har också ansvar för bl.a. den information som behandlas med stöd av it-system. Internrevisionen konstaterar med utgångspunkt från intervjuer och dokumentanalyser att informationsägarna varken genomför riskanalyser eller identifierar riskområden (och följaktligen inte heller rapporterar dessa risker i samband med övrig rapportering) i arbetet med att förebygga, upptäcka och hantera oegentligheter i de granskade it-systemen.

Bedömning
Internrevisionen konstaterar att Polismyndigheten saknar ett generellt strukturerat och enhetligt arbete mot oegentligheter samt att skrivningen i Polismyndighetens riktlinjer för intern styrning och kontroll kan vara den bakomliggande orsaken. EA har inte läm-

[10] Se PM 2017:3.
[11] Riskuppföljning T2 samt bedömningen av den interna styrningen och kontrollen inför ÅR 2017. Dnr A282.071/2017. Inte heller i redovisningen av risker för T1 eller T 2 framgår skrivning om oegentligheter. IR konstaterar med utgångspunkt från ESV: s definition att otillbörlig användning av polisens it-system är en form av oegentlighet.

nat vägledning för hur ett myndighetsövergripande och samordnat riskanalysarbete inom ramen för ISK-arbetet kan inkludera oegentlighetsrisker. I riktlinjerna pekas chefsansvaret ut för oegentlighetsarbetet men det ges inga anvisningar eller stöd för detta arbete. I sak innebär det att ansvariga chefer på egen hand får hitta lösningar för att hantera det utpekade ansvaret. Det innebär att åtgärder mot oegentligheter i allmänhet, och it-system i synnerhet, i dagsläget inte utförs systematiskt och saknar bakomliggande, grundläggande, riskanalyser. Internrevisionens bedömning är att arbetet med oegentligheter i polisens it-system bör omfattas av Polismyndighetens ISK-arbete.

Internrevisionens bedömning är att myndighetsledningen behöver få en sammantagen information om risker i polisens it-system som en del av myndighetens totala ISK-arbete. Detta innebär att EA med utgångspunkt från sitt processansvar att säkerställa en väl fungerande process för ISK behöver utveckla/förtydliga myndighetens riktlinje för intern styrning och kontroll så att den även omfattar oegentlighetsrisker.

It-avdelningen ska utifrån sitt processägaransvar för den del av verksamhets- och säkerhetsskyddet som omfattar it- och informationssäkerhet, ta fram rutiner för genomförande av riskanalyser. Utifrån framtagna rutiner kan chefer och informationsägare få ökade förutsättningar för att utöva sitt ansvar för att hantera oegentligheter i polisens it-system. Identifierade väsentliga oegentlighetsrisker i polisens it-system ska av chefer och informationsägare tertialvis rapporteras till EA som en del av myndighetens totala ISK-arbete.

Rekommendation 4.1

Röd – Mycket väsentlig brist
Internrevisionen rekommenderar att EA i egenskap av processägare enligt AO 3 kap. 19 § utvecklar/förtydligar myndighetens riktlinje för intern styrning och kontroll så att den även omfattar oegentlighetsrisker.

Konsekvensen av om rekommendationen inte följs är att Polismyndigheten i sitt ISK-arbete avviker från förordningen (2007:603) om intern styrning och kontroll. Detta kan medföra betydande negativa konsekvenser för verksamheten.

Rekommendation 4.2

Röd – Mycket väsentlig brist
Internrevisionen rekommenderar att It-avdelningen, med utgångspunkt från EA:s utvecklade ISK-riktlinje och från riktlinje PM 2017:4, tar fram en rutin för att på ett systematiskt sätt öka polisens förmåga att förebygga och upptäcka oegentligheter i polisens it-system.

Konsekvensen av om rekommendationen inte följs är att Polismyndigheten i sitt ISK-arbete avviker från förordningen (2007:603) om intern styrning och kontroll. Detta kan medföra betydande negativa konsekvenser för verksamheten.

5 Styrning, ansvars- och befogenhetsfördelning

5.1 Genomgång av styrdokument

Iakttagelse
Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it[12] beslutades i november 2017 och ersatte en rad andra beslut.[13] Av riktlinjerna framgår att ”it- och informationssäkerhet utgör en del i myndighetens övergripande arbete med intern styrning och kontroll”. Vidare framgår att det övergripande målet för Polismyndighetens informations- och it-säkerhet är ett anpassat och ändamålsenligt skydd för myndighetens informationsbehandling. Ett anpassat och ändamålsenligt skydd innebär att säkerhetsåtgärder balanseras mot faktiska risker och kostnader. Riskhantering är därför en del av den löpande verksamheten och ska ske på ett systematiskt och strukturerat sätt. Säkerhetsrisker ska utvärderas och hanteras eller accepteras. På så sätt säkerställs en riskmedvetenhet genom att de risker som myndigheten är beredda att ta är förankrade hos t.ex. ledningsgrupper, processägare, informationsägare, produktägare m.fl.

Av Polismyndighetens AO framgår det att ansvaret för informationssäkerheten är delat mellan it-avdelningen och RPCK. Detta framgår också av rikspolischefens beslut[14] om verksamhetsskyddets inriktning. Verksamhetsskyddet har ansvar för informationssäkerhet i form av text och bild och it-avdelningen ansvarar för informationssäkerhet i it-system. Av inriktningsbeslutet framgår även verksamhetsskyddets fyra målområden.[15] Ett av dessa områden är skydd av information (informationssäkerhet). Enligt AO 3 kap. 21 § är chefen för it-avdelningen processägare och avdelningen har ett verksamhetsansvar för bl.a. den del av verksamhets- och säkerhetsskyddet som omfattar it- och informationssäkerhet samt att stödja övriga avdelningar med it- och informationssäkerhet. Enligt AO 3 kap. 24 § har RPCK verksamhetsansvar för, och chefen för avdelningen är tillika processägare för, all styrning, utveckling, samordning och kontroll av verksamhetsskyddet inklusive säkerhetsskyddet, utom för de delar som it- avdelningen är ansvarig för.[16] Polismyndighetens verksamhetsskyddschef är placerad på RPCK och är tillika myndighetens säkerhetsskyddschef[17] och ska kontrollera säkerhetsskyddet.[18] Enligt AO 3 kap. 15 § har regionkanslierna inom respektive polisregion verksamhetsansvar för verksamhets- och säkerhetsskyddet inklusive informationssäkerhet, dvs. ansvar för både text, bild och information i it-system.

I sammanhanget ska också noteras ett beslut av Thomas Rolén, särskild utredare[19]. Av beslut om Polismyndighetens policy om verksamhetsskydd framgår bl.a. att information ska värderas, skyddas och finnas tillgänglig för den som är behörig när den behövs. Polismyndigheten ska också kunna identifiera och värdera risker, värdera information och tillgångar, känna till och följa gällande regler samt rapportera när något oönskat inträf-

[12] Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it, PM 2017:4. Saknr 174.
[13] Se beslut A098.091/2017 daterat 2017-11-17.
[14] A118.146/2016, daterat den 12 april 2016.
[15] Beslut för Polisens verksamhets- och säkerhetsskydd. Dnr A118.146/2016 saknr 244.
[16] Polismyndighetens AO 3 kap 24§.
[17] Polismyndighetens AO 4 kap 6§.
[18] Säkerhetsskyddsförordningen (1996:633).
[19] Polismyndighetens policy om verksamhetsskydd, PM 2015:21, från den 18 december 2014.

far. Av policyn framgår också att det till stöd för verksamhetsskyddsarbetet ska finnas ytterligare styrdokument som reglerar och visar hur verksamhetsskyddsarbetet ska utföras. Dessa ska enligt policyn finnas tillgängliga på Polismyndighetens intranät intrapolis. Internrevisionen kan dock konstatera genom intervjuer och dokumentgranskningar att det vid tidpunkten för granskningsrapporten saknas fastställda styrdokument för verksamhetsskyddets verksamhet. Beslutsinnehållet i policyn är i delar således inte överensstämmande med verkligheten.

Internrevisionen konstaterar att styrdokument motsvarande t.ex. det som rättsavdelningen (RA) tagit fram för personuppgiftsbehandlingar[20] saknas i arbetet med att förebygga och upptäcka oegentligheter i polisens it-system. Internrevisionen anser att det förra kan tjäna som ett gott exempel för det senare.

Informationsägarna har ett ansvar för den information som behandlas i ett it-system samt den information som hanteras i enlighet med gällande författningar och Polismyndighetens styrdokument. Av handläggningsordning för nationella operativa avdelningen[21] framgår att chefen för Noa är informationsägare av informationen i it-system för den brottsbekämpande verksamheten och har delegerat det ansvaret till beredningsenheten för bl.a. Rar och DurTvå samt att underrättelseenheten ansvarar för bl.a. Asp. Noa har tagit fram styrdokument i form av riktlinjer som främst berör personuppgiftsbehandlingar i bl.a. underrättelseverksamheten (Asp) och utredningsverksamheten (Rar och RurTvå). Styrdokumenten utgår från RA:s riktlinjer för den processansvariges styrdokument avseende ansvar för personuppgiftsbehandling, inte ur ett oegentlighetsperspektiv.

Enligt HR-avdelningens handläggningsordning[22] är sektionschefen för gemensam HR, arbetsgivarpolitik och avtal, informationsägare för bl.a. it-systemet Cops. HR har inte tagit fram styrdokument för informationsägarskapet för Cops. Det har framkommit i intervjuer att det råder oenighet om informationsägarskapet för informationen i Cops. HR anser att ansvaret bättre hör hemma på Noa eftersom systemet hanterar information om operativ planering, och följaktligen ligger utanför HR:s kompetensområde.

Bedömning

Internrevisionen har identifierat ett antal styrdokument och beslut av vilka det framgår ansvar för skydd av information. Granskningen visar även att det i Polismyndigheten pågår ett arbete med registervård avseende personuppgiftsbehandling. Något motsvarande arbete med inriktning på oegentligheter i allmänhet, eller med inriktning specifikt på oegentligheter i polisens it-system, har internrevisionen inte kunnat identifiera. Internrevisionen konstaterar att det saknas en tydlig och aktiv styrning och ansvarfördelning inom Polismyndigheten med inriktning på oegentligheter i polisens it-system. De olika funktionerna (it-avdelningen, verksamhetsskyddet, informationsägarna) har inte ett tydligt, direkt och uttalat ansvar för oegentligheter i it-systemen, utan det ingår mer som en diffus del av det totala ansvaret respektive funktion har att hantera. Det är därför

[20] Polismyndighetens riktlinjer för särskild registervård av personuppgiftsbehandlingar PM 2016:36, Polismyndighetens riktlinjer för den processansvariges styrdokument avseende ansvar för personuppgiftsbehandling PM 2016:37
[21] Noa 2016:148
[22] HR 2015:1.

angeläget att de olika funktionerna i samråd tar fram styrdokument för ökad enhetlighet på området och som står i samklang med Polismyndighetens AO.

Internrevisionen konstaterar också att beslut A118.146/2016, daterat den 12 april 2016, och Polismyndighetens AO 3 kap. 15 § inte är avstämda mot varandra eftersom polisregionernas verksamhetsskydd enligt AO har ansvar för informationssäkerheten, dvs. ansvar för både text, bild och information i it-systemen, medan verksamhetsskyddet på RPCK enligt beslutet endast har ansvar för informationssäkerheten för text och bild. Denna otydlighet leder enligt internrevisionen också till otydligheter i styrningen av den aktuella verksamheten.

Internrevisionens bedömning är att policyn PM 2015:21 inte står i överensstämmelse med beslut för Polisens säkerhets- och verksamhetsskydd, A118.146/2016, i vilket Polismyndigheten delat på ansvaret för informationssäkerhet, vilket inte framgår av det förstnämnda beslutet. PM 2015:21 hänvisar också till ytterligare styrdokument till stöd för verksamhetsskyddsarbetet som reglerar hur verksamhetsskyddsarbetet ska utföras. Dessa dokument ska finnas på Polismyndighetens intranät intrapolis. Internrevisionen har dock inte kunnat finna sådana dokument på intrapolis, och det har under granskningen dessutom framkommit att det saknas styrdokument. Sammantaget konstaterar internrevisionen att det finns otydligheter vad gäller olika styrdokuments existens och kopplingar till varandra.

Internrevisionens bedömning är att den nyligen framtagna och beslutade riktlinjen avseende bestämmelser för säkerhet vid informationsbehandling med stöd av it samt användning av it-system vid Polismyndigheten i huvudsak är inriktad på it-säkerhet och inte helt står i överensstämmelse med den policy som beslutades 18 december 2014 om Polismyndighetens verksamhetsskydd, PM 2015:21. Frågan kvarstår också hur och var i organisationen det övergripande informationssäkerhetsarbetet hanteras i myndigheten eftersom it-säkerhet endast utgör en delmängd av det totala informationssäkerhetsarbetet. Denna fråga granskas dock mer utförligt av internrevisionen i en annan pågående granskning.

Internrevisionens bedömning är avslutningsvis i denna del att arbetet med personuppgiftsbehandling bör tjäna som exempel för det fortsatta arbetet med att upptäcka och förebygga oegentligheter i polisens it-system. Motsvarigheten till den beskrivning av ansvarsutpekande för olika funktioner och fördelning av arbetsuppgifter dem emellan som finns i PM 2016:37 skulle kunna användas i arbetet med att upptäcka och förebygga oegentligheter i polisens it-system.

Rekommendation 5.1.1

Orange - Väsentlig brist
Internrevisionen rekommenderar att myndighetsledningen i arbetsordningen och inom ramen för befintlig organisation tar fram en systematisk process för att tydliggör styrningen, ansvarsfördelningen och processen i arbetet med att upptäcka och förebygga oegentligheter i polisens it-system.

Konsekvenserna av om rekommendationen inte följs är att det finns en risk för effektivitetsförluster i Polismyndighetens arbete med att upptäcka och förebygga oegentligheter i polisens it-system. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

5.2 Olika funktioners pågående arbete

5.2.1 It-avdelningen, it-säk, säklogg och CSL

Iakttagelse

Inom avdelningen finns CSL och logganalysteamet säk-logg är placerad på enheten it-säkerhet (it-säk) och är polisens centrala funktion för insamling, lagring och analys av loggar som visar vad användare gjort i polisens it-system (se not 2). Genom automatisk analys av inkomna loggar[23] kan polisen följa upp och kontrollera dataanvändningen på ett systematiskt sätt. ”För att garantera rättsäkerhet vid spårning, intrång och överskridandet av befogenheter måste en komplett och otvetydig logg föras över alla säkerhetsrelevanta händelser”.[24]

It-avdelningens arbete med oegentligheter i it-systemen sker i stora drag genom att säk-loggen lämnar ut begärda loggutdrag till behörig beställare eller så upptäcker säk-loggen på egen hand något avvikande som ett resultat av de regler som de själva har upprättat i CSL. I det sistnämnda fallet sker regelmässigt en anmälan till SU. Av intervjuer har det framkommit att medarbetarna vid it-säk i behörig ordning effektuerar inkomna beställningar av loggutdrag. Internrevisionen konstaterar att CSL-funktionen består av ett fåtal medarbetare som arbetar relativt självständigt under begränsad insyn. Självständigheten accentueras av att handläggarna initialt gör egna bedömningar av hur en inkommen beställning ska hanteras, t.ex. vilka analysregler i form av loggar som ska skapas. Insyn i det fortsatta arbetet finns genom att skapade loggar auditloggas för spårbarhet. Interntrevisionen har inte kunnat identifiera något styrdokument, mer än vad som följer av PM 2017:4[25], som reglerar arbetet för säk-loggen.

Vid intervjuer med medarbetare på säk-loggen har det framkommit att det saknas en struktur för att utveckla användningen av CSL-verktyget. Förutom de regelbundna mötena med SU saknas det en systematisk dialog med informationsägare och andra intressenter för utvecklingsarbete av användningen av CSL-verktyget.

Av Polismyndighetens AO framgår att varje avdelnings- och regionschef har rätt att begära loggutdrag från säk-loggen. Ytterligare behörig beställare av loggutdrag är verksamhetsskyddchefen på RPCK, regionala verksamhetsskyddchefer och personuppgiftsombudet i syfte att kontrollera personuppgiftsbehandlingen. SU får begära ut loggutdrag i samband med pågående brottsutredning och har också möjlighet att kontinuerligt bevaka och analysera it -systemen för att genom beställningar till CSL upptäcka dataintrång samt göra stickprovsanalyser.[26] Chefen för Noa har beslutat av varje enhets-

[23] Med logg menas kontinuerligt insamlad information om de operationer som utförs i ett system. En systemlogg utgörs av registrerade uppgifter om de systemoperationer som utförts och tidpunkten för dessa. Med säkerhetslogg menas logg över säkerhetskritiska händelser.
[24] Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it. PM 2017:4, sak nr 174, avsnitt 11, sidan 28.
[25] Avsnitt 11.2, sidan 28.
[26] Årsrapport 2016 Avdelningen för särskilda utredningar. A114.531/2017.

chef vid avdelningen får begära ut loggar från CSL för att kunna genomföra ålagd registervård.[27] Intervjuer ger vid handen att informationsägarna som regel beställer få loggutdrag och i synnerhet gäller detta för stickprovsbeställningar med fokus på att upptäcka eventuella oegentligheter i it-systemen. CSL-funktionen används mest frekvent av SU och verksamhetsskyddet.

5.2.2 Verksamhetsskyddet

Iakttagelse
Internrevisionens granskning visar att verksamhetsskyddet genomför aktiviteter med inriktning på skydd av information. Funktionens arbete är händelsestyrt utifrån ett säkerhetsskyddsperspektiv. Det har framkommit vid intervjuer med ansvariga för verksamhetsskyddet, på både nationell och regional nivå, att loggutdrag beställs frekvent för att utreda misstänkta oegentligheter/olämpligheter. Upptäckt och hantering av felaktigheter och olämpligheter i polisens it-system sker utifrån tips eller underrättelser. Internrevisionen konstaterar att det saknas styrdokument och systematik i arbetet (se avsnitt 5.1).

5.2.3 Sammantagen bedömning av avsnitt 5.2.1 och 5.2.2

Internrevisionens bedömning är att det finns en uppenbar risk för personberoende i säk-loggen med hänsyn till funktionens fåtaliga bemanning. Internrevisionen konstaterar också att funktionen arbetar under begränsad insyn och att det saknas styrdokument som närmare reglerar säk-loggens arbete.

Internrevisionens bedömning är att den nyligen beslutade riktlinjen för säkerhet avseende informationsbehandling med stöd av it[28] bör kompletteras med en separat aktivitetsplan som tas fram av it-säk, och som beskriver hur man avser att konkret operationalisera riktlinjens innehåll i de delar som tar sikte på rutinbeskrivningar för säk-loggens arbete med myndighetens loggdata.

Internrevisionen anser vidare att det är angeläget att möjligheterna att använda CSL utvecklas kontinuerligt och att de möjligheter verktyget erbjuder tillvaratas fullt ut för att förebygga och upptäcka oegentligheter i it-systemen. Det är därför viktigt medarbetarna vid säk-loggen ges möjligheter att vidareutveckla användningen av CSL.

Rekommendation 5.2.3.1

Orange - Väsentlig brist
Internrevisionen rekommenderar att it-avdelningen vidtar åtgärder för att minska risken för personberoende i säk-loggen samt tar fram ett styrdokument/aktivitetsplan för verksamhetens bedrivande.

[27] Arbetsordning för Polismyndigheten, PM 2017, 5 kap. 7 § 43.
[28] Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it. PM 2017:4, sak nr 174.

Konsekvenserna av om rekommendationen inte följs är att det finns en risk för effektivitetsförluster i Polismyndighetens arbete med att upptäcka och förebygga oegentligheter i polisens it-system. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

5.3 Informationsägare

Iakttagelse
Informationsägarna ansvarar enligt Polismyndighetens AO 3 kap. 16 § tredje stycket för att den information som behandlas i ett it-system hanteras i enlighet med gällande författningar och Polismyndighetens styrdokument. Informationsägarnas ansvar för innehållet i systemen kompletteras av produktägarnas ansvar för att säkerställa att produkten omgärdas av rätt säkerhet.

Internrevisionen konstaterar att Noa i egenskap av informationsägare för informationen i it-systemen Asp, Rar och Durtvå saknar kontrollaktiviteter med det primära syftet att upptäcka och förebygga oegentligheter i polisens it-system.

I informationsägarens ansvar ingår bl.a. att kvalitetsgranska uppgifter som registreras i systemet. Noa uppger att stickprovskontroller genomförs med inriktning på personuppgiftsbehandling för att säkerställa att uppgifterna i Asp registrerats enligt gällande lag.[29] Vad gäller it-systemen Rar och DurTvå har Noa tagit fram styrdokument som ger stöd för registervårdarbete med inriktning på personuppgiftsbehandling. Motsvarande aktiviteter saknas med inriktning på oegentligheter i nämnda it-system.

Internrevisionens granskning visar att HR i egenskap av informationsägare för informationen i it-systemet Cops inte bedriver något aktivt arbete med systemet. Internrevisionen har även konstaterat att det inte tagits fram styrdokument utifrån informationsägarskapet och att det saknas rutiner för registervårdsarbetet.

Intervjuer med informationsägare visar att de i delar saknar kompetens och djupare förståelse för att fullt ut effektuera sitt ansvar med avseende på informationsägarskapet och då särskilt med fokus på oegentligheter i it-systemen. Av intervjuer med säk-loggen framkommer att informationsägarna, i vart fall vad gäller de it-system som ingår i granskningen, sällan eller aldrig begär stickprovsuttag ur sina it-system med inriktning på oegentligheter.

Med anledning av genomförda intervjuer med Noa/underrättelseenheten (Noa/Und) konstaterar internrevisionen att det arbete som Noa/Und genomför inom ramen för sitt registervårdsarbete med inriktning på personuppgiftsbehandling, också har skapat en medvetenhet hos informationsägaren om dels vikten av att etablera en närmare dialog med it-avdelningen, dels skapa möjligheter till en regelbunden återkoppling mellan informationsägarna, verksamhetsskyddet, SU och GSD. Arbetssättet och slutsatserna bör överföras till att även omfatta arbetet mot oegentligheter i it-systemen.

Internrevisionen har inte kunnat identifiera strukturer för att lyfta regionala iakttagelser avseende oegentligheter i it-systemen till informationsägarna på nationell nivå. Polisens

[29] Polisdatalagen (2010:361) och personuppgiftslag (1998:204).

incidentrapporteringssystem (Point) omfattar inte, såvitt internrevisionen förstår, rapportering av oegentligheter i polisens it-system.

Bedömning
Informationsägarna ansvarar enligt Polismyndighetens AO för att den information som behandlas i ett it-system hanteras i enlighet med gällande författningar och Polismyndighetens styrdokument. Internrevisionens konstaterar dock att det hos informationsägarna saknas en djupare förståelse för vad detta ansvar innebär i sak. Internrevisionens bedömning är att it-avdelningen i egenskap av processägare för informations- och it-säkerhet[30] i större utsträckning än hittills behöver vidta åtgärder för att lämna adekvat stöd till informationsägarna med avseende på hur de ska leva upp till sitt ansvar.

För att säkerställa att befintlig information hanteras korrekt och på det sätt som är avsett och till förebyggande av oegentligheter, skulle informationsägarna med hjälp av säk-loggen kunna genomföra stickprovskontroller av användarnas hantering av information i it-systemen. I dagsläget lämnar informationsägarna förvisso stickprovsbeställningar till säk-loggen men det sker i en liten omfattning och med utgångspunkt från bestämmelserna om personuppgiftsbehandlingar. Här finns en utvecklingspotential anser interrevisionen.

Internrevisionens bedömning är också att det bör fastställas styrdokument som reglerar och ger stöd för hur informationsägare ska uppfylla ställda krav i Polismyndighetens AO. Det bör analyseras huruvida arbetet med registervård och personuppgiftsbehandling ska samordnas med oegentlighetsarbetet, där det förra kan tjäna som exempel för det senare. Internrevisionen anser att de steg mot ökat samarbete som tagits av Noa och it-avdelningen bör tjäna som ett gott exempel eller rutin för övriga informationsägare.

För att få en bra bild av myndighetens arbete med oegentligheter i polisens it-system på nationell nivå, anser internrevisionen att informationsägarna ska säkerställa att information om väsentliga oegentligheter i it-systemen rapporteras från den regionala nivån till den nationella nivån och där sammanställas av EA som en del av myndighetens ISK-arbete. Sådan rapportering ska dock endast omfatta mönster och strukturer avseende oegentligheter, inte identifierbara enskildheter. Oegentligheter som inte bedöms vara väsentliga åligger det informationsägarna själva att sammanställa och hantera inom ramen för sitt ordinarie linjeansvar.

Internrevisionens bedömning är sammanfattningsvis att informationsägarna inte bedriver något organiserat och strukturerat arbete mot att upptäcka och förebygga oegentligheter i polisens it-system.

Rekommendation 5.3.1

Orange - Väsentlig brist
Internrevisionen rekommenderar att it-avdelningen i egenskap av processägare i samverkan med informationsägarna tar fram en gemensam struktur för uppföljning av informationsägarnas åtgärder för att förebygga och upptäcka oegentligheter i polisens it-system.

[30] Polismyndighetens AO 3 kap. 21 §.

Konsekvenserna av om rekommendationen inte följs är att det finns en risk för effektivitetsförluster i Polismyndighetens arbete med att upptäcka och förebygga oegentligheter i polisens it-system. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

Rekommendation 5.3.2

Orange - Väsentlig brist
Internrevisionen rekommenderar att informationsägarna blir mer aktiva vad gäller att använda säk-loggen utifrån sitt informationsägaransvar, t.ex. bör fler och återkommande stickprovskontroller genomföras med inriktning på att förebygga och upptäcka oegentligheter av den information som behandlas i it-system.

Konsekvenserna av om rekommendationen inte följs är att det finns en risk för effektivitetsförluster i Polismyndighetens arbete med att upptäcka och förebygga oegentligheter i polisens it-system. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

Rekommendation 5.3.3

Orange - Väsentlig brist
Internrevisionen rekommenderar att it-avdelningen i egenskap av processägare enligt AO 3 kap. 21 § i samverkan med HR genomför riktade kompetensförstärkande insatser mot informationsägarna.

Konsekvenserna av om rekommendationen inte följs är att det finns en risk för effektivitetsförluster i Polismyndighetens arbete med att upptäcka och förebygga oegentligheter i polisens it-system. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

5.4 Andra angränsande funktioner i arbetet mot oegentligheter i polisens it-system

Iakttagelse

SU

Enligt förordning (2014:1106) om handläggning av ärenden om brott av anställda inom polisen och vissa andra befattningshavare ansvarar SU för att handlägga brottsanmälningar där den som påstås ha begått ett brott är anställd inom polisen eller genomgår grundutbildning till polis. SU beställer loggutdrag från CSL i sina förundersökningar och som en följd av olika underrättelser. Verksamhetsskyddet kan genomföra loggbeställningar på SU:s vägnar. SU:s samarbete med verksamhetsskyddet sker utifrån riktlinjer för SU:s verksamhet.[31]

[31] Polismyndighetens riktlinjer för handläggning av ärenden om brott av anställda inom polisen och vissa andra befattningshavare. PM 2016:49

SU anger i sin Årsrapport för 2016 att avdelningen har utvecklat den egna underrättelseverksamheten och att möjligheterna därmed har ökat att upptäcka brott mot tystnadsplikten och dataintrång. Årsrapporten beskriver även samarbetet med it- avdelningen som har ett förebyggande fokus.[32] I årsrapporten för 2016 anges också att avdelningen genom information på polisens intranät har informerat om vad som är otillåten användning av it-systemen, särskilt dataintrång genom icke tjänsterelaterade sökningar i Polismyndighetens register.[33]

Polisregionkanslierna
Vid varje regionkansli finns en grupp för skiljande- och disciplinärenden (GSD) som tar emot brottsanmälningar och förundersökningar som överlämnas från SU. Med detta som utgångspunkt beslutar GSD om en arbetsrättslig utredning ska inledas eller om ärendet ska avskrivas. GSD anmäler ärendet till personalansvarsnämnden (Pan) om det finns skäl att pröva om en arbetstagare ska skiljas från sin anställning eller meddelas disciplinpåföljd för tjänsteförseelse.[34]

I Polismyndighetens riktlinjer för handläggning av ärenden om disciplinansvar och skiljande från anställning m.m.[35] anges att: ”Det är viktigt att Polismyndigheten så långt möjligt på ett systematiskt sätt använder den kunskap och de erfarenheter som den får från bl.a. ärenden om disciplinansvar och skiljande från anställningen i ett förebyggande syfte”.

Bedömning
Internrevisionen har identifierat flera olika funktioner som var och en har ansvar för arbetet mot oegentligheter i polisens it-system. Sammanfattningsvis konstaterar internrevisionen att det saknas strukturer för samverkan mellan funktionerna och det saknas möjligheter till systematiskt och regelbundet informationsutbyte. Detta har resulterat i att de olika funktionerna i huvudsak arbetar självständigt och i stuprör utifrån det egna uppdraget.

Rekommendation 5.4.1

Orange - Väsentlig brist
Internrevisionen rekommenderar att it-avdelningen i egenskap av processägare enligt AO 3 kap. 21 § i samverkan med informationsägarna, verksamhetsskyddet, SU och GSD: - etablerar en strukturerad samverkan i syfte att skapa ökade förutsättningar för ett systematiskt arbete mot oegentligheter i polisens it-system.

Konsekvenserna av om rekommendationen inte följs är att det finns en risk för effektivitetsförluster i Polismyndighetens arbete med att upptäcka och förebygga oegentligheter i polisens it-system. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

[32] Årsrapport 2016 Avdelningen för särskilda utredningar. A114.531/2017
[33] Årsrapport 2016 Avdelningen för särskilda utredningar. A114.531/2017
[34] Polismyndighetens riktlinjer för handläggning av ärenden om disciplinansvar och skiljande från anställning m.m. PM 2016:16
[35] PM 2016:16

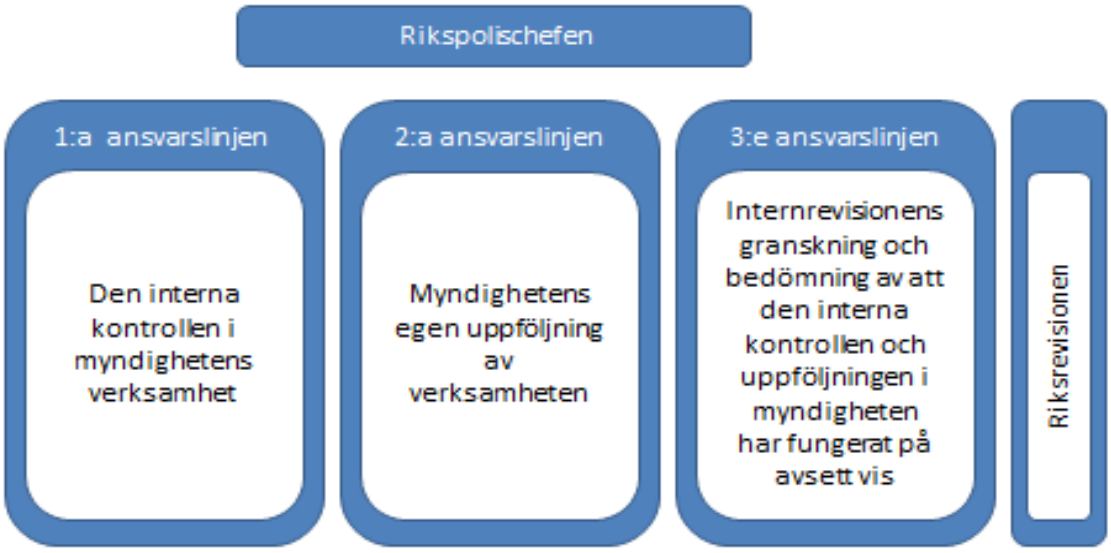
6 Sammanfattande bedömning av revisionsfrågorna

Sammanfattningsvis konstaterar internrevisionen att det i delar i Polismyndigheten saknas en process för att förebygga och upptäcka oegentligheter i polisens it-system. När det gäller att hantera sådana oegentligheter är dock förmågan ändamålsenlig genom den lagstiftning och struktur som finns inom myndigheten och som tillämpas av SU, PAN och GSD.

Arbetet med oegentligheter i polisens it-system omfattas i dagsläget inte av Polismyndighetens ISK-arbete. Internrevisionen konstaterar också att det finns en förbättringspotential avseende rutiner och intern samverkan mellan olika funktioner på området. Informationsägarna bör öka användningen av CSL genom loggutdrag och stickprovskontroller med fokus på att förebygga och upptäcka oegentligheter i sina it-system. Polismyndigheten bör genomföra kompetensförstärkande åtgärder för informationsägarna. Avslutningsvis bör myndighetens riktlinje för intern styrning och kontroll utvecklas så att den dels omfattar oegentlighetsrisker, dels utvecklar ett metodstöd för ändamålet med utgångspunkt från riktlinje PM 2017:4.

7 Sammanfattande bedömning av intern styrning och kontroll

Det finns en modell för intern styrning och kontroll som bygger på tre ansvarslinjer. Modellen används både inom privat och offentlig verksamhet. Ansvarslinjerna kan användas för att beskriva vilka som ansvarar för vad inom riskhantering och intern styrning och kontroll.



Ekonomistyrningsverket har beskrivit ansvarslinjerna på följande sätt i ”Handledning - En introduktion till den statliga internrevisionen:

”Den första ansvarslinjen är myndighetens dagliga verksamhet och processer. I myndigheten ska det finnas en god intern kontroll i samtliga delar av den operativa verksamheten. Ansvar och befogenheter ska vara tydliga. Den interna kontrollen ska förebygga fel, avsiktliga eller oavsiktliga, i det som myndigheten gör. Handläggare och chefer är en del i den här ansvarslinjen. Funktioner i den första ansvarslinjen ansvarar för

att hantera risker och upprätthålla en effektiv intern styrning och kontroll. Att upprätthålla en hållbar riskkultur är första linjens ansvar.

I den andra ansvarslinjen ligger myndighetens regelbundet återkommande uppföljning och efterkontroller. Chefer, controllers och funktioner som arbetar med risker är en del i den här ansvarslinjen. Uppföljning och efterkontroller görs även av andra funktioner och i olika sammanhang – med andra ord kan många personer ingå i andra ansvarslinjen. Exempelvis personer i stödverksamheten som arbetar med uppföljningar och utvärderingar i ett bredare perspektiv.” Den andra ansvarslinjen är mer funktionellt orienterad. Här avses funktioner som arbetar specifikt med att övervaka risktagande. Dessa funktioner bidrar till att utveckla processer kring intern styrning och kontroll men de har även ansvar för att övervaka första linjens arbete.

Den tredje ansvarslinjen utgörs av internrevisionsfunktionen som arbetar på ledningens uppdrag och granskar första och andra linjens arbete.

Kvaliteten i arbetet i ansvarslinjer påverkar varandra ömsesidigt. Föreligger brister i arbetet med intern styrning och kontroll i första ansvarslinjen leder det inte bara till en högre risk för myndigheten, utan det påverkar även arbetet i andra och tredje ansvarslinjen på ett negativt sätt, t.ex. genom att uppföljning och utvärdering blir onödigt resurskrävande och felfokuserat. Hög kvalitet i riskhanteringen i första ansvarslinjen kan innebära att andra och tredje ansvarslinjen kan arbeta mer proaktivt.

På motsvarande sätt leder brister i andra ansvarslinjen till sämre total riskhantering. Om den andra ansvarslinjen är outvecklad och inte stödjer organisationen med bra styrmedel, modeller och ramverk försvåras första ansvarslinjens riskhanteringsarbete.

I vilken utsträckning ansvarslinjerna är effektiva beror till står del på deras förmåga att samverka kring riskhantering och intern styrning och kontroll.

Internrevisionen har i denna granskning av intern styrning och kontroll av polisens förmåga att förebygga, upptäcka och hantera oegentligheter i polisens it-system använt ovanstående modell för att göra en sammanfattande bedömning. Internrevisionen har sett följande ansvarslinjer:

- linje 1: informationsägarna: äger informationen i it-systemen och hur den ska behandlas
- linje 2:
    - it-avdelningen: ansvarar för att styra och leda it-och informationssäkerhetsarbetet inom Polismyndigheten
    - EA: har ett samordnande ansvar för Polismyndighetens rapportering av den interna styrningen och kontrollen
    - verksamhetsskyddet: enligt Polismyndighetens AO 3 kap. 15 § har regionkanslierna inom respektive polisregion verksamhetsansvar för verksamhets- och säkerhetsskyddet inklusive informationssäkerhet, dvs. ansvar för både text, bild och information i it-systemen
    - GSD: tar emot brottsanmälningar och förundersökningar som överlämnas från SU och med detta som utgångspunkt beslutar GSD om en arbetsrättslig utredning ska inledas eller om ärendet ska avskrivas

- SU/und (är med utgångspunkt från sitt uppdrag självständiga i förhållande till andra aktörer i Polismyndigheten) .

Internrevisionens bedömning är att det finns en utvecklingspotential när det gäller kompetens och förståelse för vad det innebär att vara informationsägare beträffande första ansvarslinjen (Noa och HR) och att det är nödvändigt att genomföra kompetensförstärkande åtgärder för att öka förmågan att genomföra riskanalyser och kontrollaktiviteter.

Internrevisionens bedömning är att det saknas en tydlighet i ansvarsfördelning och befogenhet, det saknas också en strukturerad samverkan beträffande första ansvarslinjen (informationsägarna) och delvis andra ansvarslinjen (it-avdelningen och verksamhetsskyddet).

I andra ansvarslinjen saknas riskanalyser och uppföljning av identifierade risker. Internrevisionen konstaterar också att det i denna ansvarslinje saknas en process för att förebygga, upptäcka och hantera oegentligheter i polisens it-system samt att arbetet med oegentligheter i polisens it-system i dagsläget inte omfattas av Polismyndighetens ISK-arbete.

Internrevisionens sammanfattande bedömning är att den interna styrningen och kontrollen avseende polisens förmåga att förebygga, upptäcka och hantera oegentligheter i polisens it-system har ett antal brister. Bristerna avser främst förmågan att upptäcka och förebygga oegentligheter i polisens it-system. Bristerna förekommer både i första- och andra ansvarslinjerna vilka därför behöver ses över.

Philip Jansson Marja Seppänen Winfred Nionzima

Polisen
Polismyndigheten

Beslutsprotokoll

Datum	Beslutsnummer
2019-03-26	RPC 52/2019
Diarienr, ärende	Saknr
A419.644/2016	977

Beslutande	Föredragande
Rikspolischefen Anders Thornberg	Polisintendenten Stefan Eurenius

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

Ärende
Beslut om åtgärder med anledning av internrevisionens granskning av polisens förmåga att förebygga, upptäcka och hantera oegentligheter i Polismyndighetens it-system.

Beslut
Internrevisionen har genomfört en granskning av polisens förmåga att förebygga, upptäcka och hantera oegentligheter i Polismyndighetens it-system.

It-avdelningen, ekonomiavdelningen och rättsavdelningen har lämnat förslag till åtgärder med anledning av rekommendationerna. Delar av internrevisionens rekommendationer kommer vidare att tas om hand i arbetet med att omhänderta de förslag som har lämnats i utredningen om Polismyndighetens verksamhets- och säkerhetsskydd (dnr A365.948/2018).

Polismyndigheten beslutar följande.

Rekommendation 4.1
Ekonomiavdelningen ska förtydliga och uppdatera Polismyndighetens riktlinjer för intern styrning och kontroll avseende oegentlighetsrisker. Chefen för ekonomiavdelningen är ansvarig för arbetet. Åtgärdena ska vara genomförda senast den 30 september 2019.

Rekommendation 4.2
It-avdelningen ska ta fram en rutin för stickprovskontroller avseende de granskade it-systemen ASP (allmänna spaningsregistret), Durtvå (datoriserad utredningsrutin med tvångsmedel) och Cops (centralt operativt planeringssystem) i syfte att öka Polismyndighetens förmåga att förebygga och upptäcka oegentligheter i Polismyndighetens it-system. Därutöver ska it-avdelningen ta fram en plan för hur likartade rutiner ska införas för övriga it-system.

Vidare ska it-avdelningen etablera ett samverkansforum för it-avdelningen, verksamhetsskyddet, avdelningen för särskilda utredningar och informationsägare i syfte att förbättra förmågan att upptäcka oegentligheter.

It-avdelningen ska också ta fram ett utbildningspaket för informationsägare avseende centrala säkerhetsloggen.

Ansvarig är chefen för it-avdelningen och åtgärderna ska vara genomförda under andra kvartalet 2019.

Rekommendation 5.1.1
Av arbetsordningen ska det framgå att processägare ansvarar för intern styrning och kontroll av den information som inom dennas ansvarsområde behandlas i it-system. Rättsavdelningen ska säkerställa att ansvarsfördelningen avseende styrningen av Polismyndighetens informationssäkerhetsarbete tydliggörs i arbetsordningen.

Chefen för rättsavdelningen ansvarar för åtgärdernas genomförande. Åtgärderna ska vara genomförda senast den 1 september 2019 i samband med att årets ändringar av arbetsordningen träder i kraft.

Vid genomförandet av de beslutade åtgärderna ska Polismyndighetens skyldigheter vid hantering av personuppgiftsincidenter och andra relevanta krav i dataskyddsregleringen beaktas.

Rekommendation 5.2.3.1
Ingen åtgärd kommer att vidtas med anledning av rekommendationen. It-avdelningen bedömer att säkerhetsloggen är rätt bemannad utifrån nuvarande arbetsbelastning.

Rekommendation 5.3.1
Rekommendationen omhändertas under punkt 4.2.

Rekommendation 5.3.2
Rekommendationen omhändertas under punkt 4.2.

Rekommendation 5.3.3
It-avdelningen ska ta fram ett utbildningspaket för informationsägare avseende centrala säkerhetsloggen och genomföra riktade kompetenshöjande åtgärder. Åtgärderna ska vara genomförda senast den 31 december 2019.

Rekommendation 5.4.1
Rekommendationen omhändertas under punkt 4.2.

Kostnad	Finansiering

Vid protokollet

Stefan Eurenius

Justeras

Anders Thornberg

Sändlista	Kopia till
Samtliga avdelningar och polisregioner	Arbetstagarorganisationerna Skyddsorganisationen