



# **Granskning av den it-forensiska verksamheten**

Internrevisionen

2020-09-28

## Granskning av den it-forensiska verksamheten

### INNEHÅLL

<b>1</b>	<b>SAMMANFATTNING</b> .....	<b>3</b>
<b>2</b>	<b>INLEDNING</b> .....	<b>4</b>
2.1	Bakgrund.....	4
2.2	Syfte och revisionsfrågor .....	5
2.3	Verksamhet som ingått i granskning.....	5
2.4	Avgränsning.....	5
2.5	Informationsinsamling och metod .....	6
2.6	Bedömningsgrunder.....	6
<b>3</b>	<b>STYRNING OCH ANSVAR</b> .....	<b>6</b>
3.1	Processansvar och samverkan.....	6
3.2	Styrdokument och metodutveckling .....	9
<b>4</b>	<b>DEN IT-FORENSISKA VERKSAMHETEN</b> .....	<b>11</b>
4.1	Etablering av de regionala it-brottscentrum, RC3.....	11
4.2	Resursdimensionering personal .....	12
4.3	Verksamhetsansvaret hos NFC och RC3 .....	14
4.3.1	Förmågor .....	14
4.3.2	Dialogen UL och it-forensik.....	14
4.3.3	Beställningar från utredningsverksamheten .....	15
4.3.4	Ärendehantering inom RC3.....	15
4.3.5	Leveranserna till utredningsverksamheten.....	16
4.3.6	Bedömning samtliga avsnitt under 4.3.....	16
4.4	Informationsförvaltning, arkiv och gallring.....	18
<b>5</b>	<b>IT-SYSTEM, IT-TJÄNSTER, IT-INFRASTRUKTUR</b> .....	<b>19</b>
<b>6</b>	<b>KOMPETENSFÖRSÖRJNING OCH KOMPETENSUTVECKLING</b> .....	<b>22</b>
6.1	Kompetens .....	23
6.2	Rekrytering, bemanning och lönebildning.....	24
6.3	Interna utbildningar.....	24
<b>7</b>	<b>SAMMANFATTANDE BEDÖMNING AV REVISIONSFRÅGORNA</b> .....	<b>26</b>

### BILAGOR

Beslutsprotokoll RPC 2020-09-28

## 1 Sammanfattning




Granskningen har utförts i enlighet med revisionsplanen för 2019-2020. Syftet har varit att bedöma den interna styrningen och kontrollen av den it-forensiska processen. Internrevision gör den övergripande bedömningen att det finns förbättringsmöjligheter vad gäller styrningen av den it-forensiska verksamheten. Polismyndigheten har genomfört ett antal åtgärder för att förbättra styrningen. Det finns numera ett samverkansråd, med syfte att ensa, effektivisera och utveckla Polismyndighetens förmåga rörande brott med it-relevans med fokus på it-forensik. Det är internrevisionens uppfattning att den it-forensiska verksamhetens organisationsstruktur kommer ha utmaningar och att gränsdragningar till viss del alltid kommer att finnas. Det är därför viktigt att processägare säkerställer att samverkansarbetet fortskrider och att arbetet löpande utvärderas så att ”skav” kan identifieras och omhändertas.

De övergripande frågorna i processansvaret har varit eftersatta, vilket har resulterat i att verksamheten inte maktat med att prioritera forskning och utveckling, metodutveckling, framtagande av styrdokument samt att arbeta fram ett enhetligt och systematiskt arbetssätt. Internrevisionens bedömning är att den it-forensiska verksamheten inte har tillräckligt med personella resurser. Det är viktigt att resursdimensionering av den it-forensiska verksamheten görs och utgångspunkten är utredningsverksamhetens behov av it-forensiskt stöd. Internrevisionen anser vidare att NFC bör säkerställa att det avsätts tillräckliga resurser för att processägarskapet kan fullföljas i enlighet med arbetsordningen. NFC bör i egenskap av processägare utvärdera vilket resursbehov som finns för att avdelningen ska kunna säkerställa att resultat uppnås inom den it-forensiska verksamheten.

Internrevisionens bedömer att behovet av it-stöd för it-forensik, både för it-forensiker och utredare, inte har tillgodosetts tillräckligt. Den it-forensiska verksamheten är i hög grad beroende av it-stöd, vilket gör att myndigheten behöver fastställa vilken teknisk kapacitet som ska finnas för att möta efterfrågan i utredningsverksamheten.

Det finns även förbättringsmöjligheter beträffande kompetensförsörjnings- och kompetensutvecklingsområdet. Den it-forensiska verksamheten är it-intensiv och it-kompetens behöver förstärkas. Avsaknad av it-forensik som ämne vid den polisiära grundutbildningen har medfört bristande grundkompetens vad gäller it-forensik i kärnverksamheten. Interna utbildningar måste prioriteras för att hantera skillnader i kompetens hos befintlig personal men även för att möjliggöra kvalitativ internrekrytering. Det saknas en tillräcklig nivå på kandidater med it-forensisk kompetens på marknaden, både den privata och offentliga. Polismyndigheten behöver samverka bättre med utbildningsäten för att ta fram nya utbildningar.

Tabellen nedan visar att internrevisionens granskning har resulterat i totalt 12 rekommendationer, fördelade utifrån internrevisionens modell för bedömning av brister som presenteras i rapporten.

	<b>Antal</b>
 Mycket väsentlig brist	3
 Väsentlig brist	9
 Mindre väsentlig brist	-

## 2 Inledning

Granskningen har utförts i enlighet med revisionsplanen för 2019-2020.

### 2.1 Bakgrund

Enligt arbetsordningen är nationella operativa avdelningen (Noa) processansvarig för huvudprocessen utredning och lagföring<sup>1</sup>. Nationellt forensiskt centrum (NFC) är processansvarig för den it-forensiska processen<sup>2</sup>. It-forensisk verksamhet utförs i den it-forensiska processen och stödjer utredningsprocessen<sup>3</sup>. Vid Noa finns nationellt it-brottscentrum som arbetar enligt den it-forensiska processen. Noa är processansvarig för de fem processer som jämte it-forensik utförs vid nationellt och regionala it-brottscentrum: komplexa cyberbrott, internetrelaterade sexuella övergrepp mot barn, internetinhämtning, särskild internetinhämtning utredning och it-relaterade brott<sup>4</sup>. Det finns därmed gränssytor mellan Noa och NFC vad gäller den it-forensiska processen.

Under 2013 etablerade EU vid Europol ett europeiskt Cybercrime Centre (EC3) som utgör noden i Europas brottsbekämpning av den nationsgränslösa cyberbrottsligheten. I oktober 2015 beslutade Polismyndigheten att det skulle inrättas ett nationellt it-brottscentrum - Swedish Cybercrime Centre (SC3) - vid Noa. Syftet var att samla resurser och processer för att kunna bygga upp specialistkompetens och samordna arbetet mot it-relaterade brott. I maj 2016 fick SC3 uppdraget att ta fram förutsättningar för ett enhetligt arbetssätt på nationell och regional nivå för brott med it-relevans. 2017 fattades beslut om att inrätta regionala it-brottscentrum (RC3) i samtliga regioner. Ett första steg var att det senast den 31 mars 2017 skulle finnas en samordningsfunktion för ärenden som avser brott med it-relevans.

I juni 2018 fattade chefen för Noa beslut om inriktning av resursdimensionering och ambitionsnivå för att inrätta regionala it-brottscentrum. I september 2018 fattade rikspolischefen beslut om fördelning av medel till regionala it-brottscentrum 2019-2020. Idag finns ett beslut avseende ansvarsfördelning och samverkan mellan NFC, SC3 och polisregionerna.

Brå genomförde en studie avseende it-inslag i brottsligheten och rättväsendets förmåga att hantera dem<sup>5</sup>. Vid intervjuer i internrevisionens planeringsarbete för denna granskning framkom att flertalet av bristerna i rapporten uppfattas vara kvarstående. Brås rapport visade att de satsningar som hade gjorts på it-området inte motsvarade behovet. Det ansågs ytterst angeläget att Polismyndigheten skulle tillsätta de resurser som krävdes för att såväl kompetens- som kapacitetshöjande åtgärder kunde genomföras. Det uttrycktes även vikten av att de åtgärder som skulle genomföras inte blev en engångssatsning, utan att satsningarna på it-området fortlöper och uppdateras i takt med utvecklingen. I riksrevisionens rapport It-relaterade brottslighet – Polis och åklagare kan bli effektivare<sup>6</sup> framgick bland annat att: bristen på vedertagna metodstöd, utvecklade arbetssätt, till-

<sup>1</sup> PM 2019:23, 3 kap 4 §.

<sup>2</sup> PM 2019:23, 3 kap 19 §.

<sup>3</sup> PM 2020:18 Riktlinjer för den it-forensiska verksamheten.

<sup>4</sup> Noa 2016:148.

<sup>5</sup> Brå Rapport 2016:17.

<sup>6</sup> RiR rapport 2015:21.

räcklig kompetens och specialisering inom området gjorde att polis och åklagare inte hade beredskap och förmåga att utreda och handlägga it-relaterade brott på ett effektivt och ändamålsenligt sätt. Internrevisionen noterade inledningsvis att inrättande och etablering av SC3 och de regionala RC3 har lett till framsteg i Polismyndighetens it-forensiska verksamhet och hantering av it-brottsligheten.

## 2.2 Syfte och revisionsfrågor

Syftet har varit att bedöma den interna styrningen och kontrollen av den it-forensiska processen. Målet med granskningen har varit att bedöma om den it-forensiska verksamheten bedrivs effektivt enligt myndighetsförordningens 3 §.

Följande revisionsfrågor har ingått i granskningen:

1. Hur fungerar styrningen (organisation, ansvar, roller, styrdokument, resurser, beroende till stödprocesser, etc.) av den it-forensiska verksamheten?
2. Hur tillgodoses den it-forensiska verksamhetens behov av it-tjänster, it-system och it-infrastruktur?
3. Hur tillgodoses kompetensförsörjnings- och kompetensutvecklingsarbetet vad gäller it-forensik som ett stöd för utredningsprocessen?

## 2.3 Verksamhet som ingått i granskning

- NFC - utifrån processansvar för den it-forensiska processen.
- Noa - utifrån processansvar för utredningsverksamheten och SC3 utifrån främst Noas ansvar för det fortsatta arbetet med etableringen av RC3.
- Regionerna - ledning och styrning av it-forensiska verksamheten och RC3:orna.
- HR-avdelningen - utifrån processansvar för rekrytering, lönebildning, kompetensförsörjning och kompetensutveckling.
- It-avdelningen (it) - utifrån processansvar för bland annat att tillhandahålla it-tjänster samt utveckla, förvalta och sköta drift av it-system och it-infrastruktur.
- Representanter i samverkansrådet för it-forensik (NFC, Noa, it, HR).
- Rättsavdelningen (RA) – utifrån processansvar för informationsförvaltning och arkivering.

## 2.4 Avgränsning

I uppdragsbeskrivningen gjorde internrevisionen bedömningen att verksamheten som bedrivs av SC3 och som inte är en del av den it-forensiska processen inte ska ingå i granskningen. Dock har granskningens iakttagelser övergripande berört verksamheten inom Noa och SC3 med avseende på gränsdragning av processansvaret för it-forensik. Internrevisionen har inte granskat it-forensik inom ramen för verksamhetsansvaret hos SC3.

## 2.5 Informationsinsamling och metod

Granskningen har omfattat genomgång och analys av styrdokument, beslut, rapporter samt annan relevant dokumentation. Intervjuer har genomförts med olika befattningshavare inom NFC sektionen för Informationsteknik, regionala RC3, Noa SC3, regionala utredningsenheter, it, HR, EA. Bland annat har följande funktioner ingått: it-forensiker, gruppchefer inom it-forensik, processledare, verksamhetsutvecklare, utredare inom RC3, utredare och FU-ledare i polisregioner samt andra relevanta funktioner utifrån granskningens uppdrag. De regionala RC3 som inte besökts/intervjuats har internrevisionen haft kortare skriftlig avstämning via mail kring ett antal övergripande frågor.

Granskningen har utförts under perioden september – december 2019 av internrevisorerna Winfred Nionzima (ansvarig revisor) och Lars Agerberg. Kommissarie/sektionschef Kent Drougge har varit sakkunnig i granskningen. Rapporten sakgranskades mars-april 2020 av NFC, Noa/SC3, samtliga polisregioners RC3, EA, IT, HR samt RA. Begäran om inhämtande av åtgärdsförslag skickades till RPC kansli 2020-04-20. Åtgärder återges i beslutsbilaga till rapporten.

## 2.6 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 Styrning och ansvar

### 3.1 Processansvar och samverkan

#### Iakttagelser

NFC har processansvar för den it-forensiska processen som bedrivs inom hela Polismyndigheten. It-forensisk verksamhet bedrivs vid Polismyndighetens samtliga polisregioner, vid Noa och NFC. Vid regionerna är den it-forensiska verksamheten organiserad som en spegling av verksamheten vid SC3 och består av funktionerna: desk, internetinhämtning, internetrelaterade sexuella övergrepp mot barn (Isöb), komplexa cyberbrott samt it-forensik. It-forensiska funktionerna vid RC3 ska stödja både den utredningsverk-

samheten som bedrivs vid RC3 och all övrig utredning inom regionen där it-forensiskt stöd krävs. I avsnitt 6 Ansvarsområden i riktlinjerna för it-forensisk verksamhet<sup>7</sup> framgår ett förtydligande av ansvarsfördelning mellan de olika aktörerna som bedriver it-forensisk verksamhet inom Polismyndigheten.

Enligt arbetsordningen innebär processansvar ett nationellt ansvar för en viss process inom hela myndigheten och för att processen säkerställer att resultat uppnås inom verksamheten. Den som har processansvar är processägare. I en processägars processansvar ingår bland att:

- beskriva processen, dess syfte och avgränsning
- kartlägga beroenden till andra processer
- besluta om processen, uppdatera och utveckla styrdokument
- säkerställa enhetlighet
- stödja arbetet i processen
- utveckla processen genom att uppmärksamma förändringsbehov och initiera förbättringsarbete
- följa upp processen bl.a. genom att mäta hur effektiv den är för att nå uppsatta mål
- ansvara för kravställningen i processerna för utbildning, inköp av varor, tjänster och lokaler<sup>8</sup>.

Vid intervjuer har framkommit att NFC inte är tillräckligt bemannad för att bedriva det arbete som åligger avdelningens processansvar för det it-forensiska arbetet. Orsakerna har uppgetts vara flera men en avgörande faktor som återkommit är att NFC:s sektion för informationsteknik inte blev rätt resursdimensionerad i omorganisationen. Inom ramen för budgetrevidering tertial 1 år 2018 beslutade Polismyndigheten om utökad budget till de regionala it-brottcentrum för åren 2019-2020. Syftet var att regionerna skulle få extra budgetmedel för att etablera RC3. NFC var en av de aktörerna involverade i den it-forensiska verksamheten som inte fick inte någon utökad budget. Vid budgetrevideringen pågick samtidigt diskussioner om huruvida SC3 eller NFC skulle få processansvar för it-forensik. Enligt uppgift kan detta ha påverkat att ingen dialog pågick, vare sig från NFC eller SC3, om att få extra budgetmedel för att axla processansvaret för it-forensik. Det har framkommit att det inom NFC pågår en budgetdialog avseende resurs- och bemanningsfrågorna när det gäller den kortsiktiga och långsiktiga planeringen för it-forensisk verksamhet. De ansvarsområden som bland annat berör forskning och utveckling (FoU), omvärldsbevakning, metodutveckling och framtagande av styrdokument och utbildningsfrågor har NFC inte mäktat med fullt ut. Prioritering har varit att biträda med it-forensisk avancerad och specialiserad kompetens vid de utredningar som bedrivs av RC3 eller SC3. Det har uppgetts att samhällsutvecklingen med snabb it-utveckling och avancerad it-brottslighet samt den grova brottsligheten har lett till ett högt tryck på den it-forensiska verksamhetens handläggningskapacitet. Uppföljning och utvärdering av det it-forensiska stödet i utredningsverksamheten uppges vara eftersatt och i granskningen har framkommit att NFC saknar tillräcklig kapacitet att genomföra ett uppföljningsarbete utifrån processansvaret.

<sup>7</sup> PM 2020:18.

<sup>8</sup> PM 2019:23, 3 kap 3 §.

Noa:s beslut<sup>9</sup> avseende ansvarsfördelning och samverkan mellan NFC, SC3 och polisregionerna har legat till grund för det arbete som bedrivits i samverkansforumet för den it-forensiska verksamheten. Genom NFC beslut<sup>10</sup> fastställdes riktlinjer för samverkansrådet för it-forensik. Samverkansrådets syfte är att ensa, effektivisera och utveckla Polismyndighetens förmåga rörande brott med it-relevans med fokus på it-forensik. Detta ska ske i samråd med ansvariga för berörda processer. Ansvariga enheter ska samarbeta bland annat avseende utbildningsfrågor, metodutveckling, framtagande av styrdokument och kravställning för it-stöd. Samverkansarbetet har uppgetts fungera bättre än tidigare men det har under granskningens genomförande uppgetts att viss oenighet fortfarande funnits avseende gränsdragning och ansvarsfördelning. Under tiden för internrevisionens genomförande av granskningen har samverkansarbetet bedrivit ett intensivt arbete med framtagande av riktlinjer, kravställning för utbildningar och it-stöd.

Det har framkommit att NFC inte kunnat bidra med tillräckliga personella resurser utifrån sitt processansvar. Under granskningens färdigställande har arbetet med riktlinjer för den it-forensiska verksamheten hunnit slutföras. Från vissa parter har framförts att den tidigare oenigheten nu har minskat och samtliga involverade aktörer är nu överens om en it-forensisk verksamhet. Enligt riktlinjerna innebär it-forensisk verksamhet att i brottsutredningar planera, säkra, extrahera, analysera och värdera digitala spår från elektroniska enheter eller källor.

### Bedömning

Det är viktigt att NFC och Noa på processägarnivå arbetar nära varandra för att identifiera aktiviteter som ska genomföras för att uppfylla målen i Polismyndighetens strategiska verksamhetsplan 2020-2024 (det långsiktiga målet *framgångsrik brottsbekämpning och uppklaring* samt *delmålet färre medborgare utsätts för brott och fler brott klaras upp*). Internrevisionens bedömning är att den it-forensiska verksamheten är eftersatt. Polismyndigheten har dock utifrån rapporter från Brå och RiR vidtagit åtgärder som bidragit till förbättringar. En rad beslut har fattats av Noa när det gäller inrättande av polisregioners RC3 samt finns det numera en överenskommelse om samverkan mellan olika parter. Polismyndigheten har vid budgetrevideringar beslutat om utökad tilldelning av medel till de regionala it-brottscentrum. Dock fick inte NFC någon utökad budget. Internrevisionens bedömning är att NFC bör säkerställa att det avsätts tillräckliga resurser för att processägarskapet kan fullföljas i enlighet med arbetsordningen. NFC bör i egenskap av processägare utvärdera vilket resursbehov som ska finnas för att avdelningen ska kunna säkerställa att resultat uppnås inom den it-forensiska verksamheten. Internrevisionen bedömer vidare att NFC behöver tillse att avdelningen har tillräcklig och rätt utredningskompetens för att kunna hantera processägarskap av it-forensisk som en stödjande process till utredningsverksamheten. NFC bör i samråd med SC3 och polisregioners RC3 kartlägga vilket it-forensiskt arbete som behöver genomföras utifrån utredningsverksamhetens efterfråga för it-forensiskt stöd.

Flera av de övergripande besluten som fattats rörande it-forensik (inrättande av RC3, resursdimensionering, beslut om ansvarsfördelning och samverkan) har fattats av Noa. De senare besluten om samverkansrådet samt riktlinjerna har fattats av NFC. För klargörande av gränsdragning mellan processansvaret för it-forensisk processen och it-

<sup>9</sup> Beslutsprotokoll Noa 61/2018.

<sup>10</sup> Beslutsprotokoll NFC A008.734/2018.



relaterade brottslighet är det viktigt att det fortsättningsvis är tydligt med var organisatoriskt beslut fattas.

Internrevisionens bedömning är att aktörerna som är ansvariga för den it-forensiska verksamheten har bedrivit ett framgångsrikt samverkansarbete som lett till att gränsdragningar kring ansvarsfördelning för it-forensik låsts upp. Det har fastställts en definition av it-forensik, var i myndigheten it-forensisk verksamhet bedrivs och ansvarsfördelning är tydliggjord. Det är internrevisionens uppfattning att den it-forensiska verksamhetens organisationsstruktur kommer ha utmaningar och att gränsdragningar till viss del alltid kommer att finnas. Det är därför viktigt att processägare säkerställer att samverkansarbetet fortskrider och att arbetet löpande utvärderas så att skav kan identifieras och omhändertas.

## Rekommendationer

### *Rekommendation 3.1.1*

#### **Röd – Mycket väsentlig brist**

Internrevisionen rekommenderar att NFC säkerställer att det avsätts tillräckliga resurser för att processägarskapet för den it-forensiska verksamheten ska bedrivas och fullföljas i enlighet med arbetsordningen.

Konsekvensen av om rekommendationen inte följs är att den it-forensiska verksamheten styrs och bedrivs ineffektivt. Bristerna har en allvarlig påverkan på Polismyndighetens förmåga att uppnå målen för en framgångsrik brottsbekämpning och uppkläring. Detta kan innebära stora negativa konsekvenser för Polismyndighetens verksamhet med avseende på myndighetsförordningens krav på effektivitet och lagenlighet.

### *Rekommendation 3.1.2*

#### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att processägare för den it-forensiska processen säkerställer att samverkansarbetet för den it-forensiska verksamheten löpande utvärderas.

Konsekvensen av om rekommendationen inte följs är att samverkansarbetet för den it-forensiska verksamheten inte bedrivs på ett ändamålsenligt sätt vilket har negativ inverkan på hur processansvaret bedrivs. Detta kan medföra betydande negativa konsekvenser för Polismyndighetens utredningsverksamhet och innebära att verksamheten inte bedrivs effektivt.

## 3.2 Styrdokument och metodutveckling

### Iakttagelser

Den it-forensiska verksamheten som bedrivs i myndigheten har saknat övergripande styrdokument i form av riktlinjer. Det har även framkommit att det saknats metodstöd såsom rutinbeskrivningar för olika ämnesområden inom it-forensik och som används och tillämpas enhetligt i polisregioners RC3 verksamheter. Det har förekommit att regionala stöddokument tagits fram som i vissa fall delats och tillämpats i regionerna. NFC har uppgett att det finns framtagna styrdokument för områden dekryptering, multimedia, mobil, data och elektronik men att dessa endast fastslagna på NFC och är inte omarbetade till styrdokument enligt Polismyndighetens format. Under granskningens genomfö-

rande har NFC tillsammans med Noa och polisregionerna tagit fram riktlinjer för den it-forensiska verksamheten.

Inom NFC finns standardiserade metoder/best practice som följer ISO-standards. För den laborativa verksamheten har det uppgetts finnas formaliserade metoder och ramar för arbetet. Det har vid intervjuer med NFC framkommit att styrdokumenterna inom avdelningen inte är kompletta samt att det finns behov av förankring i den it-forensiska verksamheten där de ska tillämpas.

Intervjuer med utredningsverksamheten samt en representant för utveckling av metodstödet Polisens nationella utredningsdirektiv (PNU) visar att det finns behov av att utveckla metodstödet i de delar som rör it-forensik. Det uppfattas inte finnas tillräckligt stöd för utredningsverksamheten när det gäller hur it-forensik ska användas i brottsutredningar. Ett arbete pågår med framtagande av en utredningsstrategi där en förmåga som avser it-forensik ska formuleras. Avsikten är att det sedan sker en koppling till PNU. När det gäller polisens metodstöd för utredning av grova brott (PUG) finns angivet att it-forensiker regelmässigt bör medverka vid såväl planering som genomförande av husrannsakan<sup>11</sup>.

Det har vidare framkommit att den it-forensiska verksamheten är it-intensiv och att utveckling inom it-området sker snabbt. Detta gör att metodutveckling och befintliga arbetssätt behöver anpassas kontinuerligt. Det har uppgetts att myndigheten inte har haft förmåga och kapacitet att arbeta med metodutveckling i tillräcklig omfattning vilket har resulterat i att området med styrdokument och metodutveckling blivit eftersatt.

Internrevisionen har tagit del av riktlinjerna för den it-forensiska verksamheten och noterat att dokumentet beskriver den it-forensiska verksamheten på en övergripande nivå. Flera områden som internrevisionen identifierat som oklara täcks in av riktlinjerna. Internrevisionen kan konstatera att stora delar av beskrivningen av den it-forensiska verksamheten i riktlinjerna är mer av en målbild än en beskrivning av verkligheten.

### **Bedömning**

Internrevisionen anser att den it-forensiska verksamheten saknar effektiva styr- och stöddokument för sin verksamhet. Prioritering av framtagande av styrdokument och metodutveckling har inte kunnat ske på grund av bland annat avsaknad av resurser. Den nationella och övergripande styrningen har skett genom enskilda beslut. Internrevisionen anser att det är positivt att det nu finns riktlinjer för den it-forensiska verksamheten. Dock kan internrevisionen konstatera att det återstår arbete med framtagande av ytterligare styrdokument och metodutveckling. Exempel på detta är metodstöd såsom handböcker och rutinbeskrivningar för de olika ämnesområdena inom it-forensik. I detta arbete bör det även identifieras vilka metodstöd som behövs för utredningsverksamheten. Det är av stor vikt att det finns styrdokument som fastställer ett systematiskt arbetssätt som kan bidra till ett enhetligt, effektivt och rättsäkert arbete.

---

<sup>11</sup> PUG avsnitt 11.2.2, version 4, september 2017.

### **Rekommendation 3.2.1**

#### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att processägare för den it-forensiska processen tar fram nödvändiga styr- och stöddokument för den it-forensiska verksamheten. Styr- och stöddokument för den it-forensiska processen som ingår i utredningsverksamheten ska också tas fram.

Konsekvensen av om rekommendationerna inte följs är att den it-forensiska verksamheten inte bedrivs strukturerat och enhetligt. Detta kan medföra betydande negativa konsekvenser för Polismyndighetens utredningsverksamhet och innebära att verksamheten inte bedrivs effektivt.

## **4 Den it-forensiska verksamheten**

### **4.1 Etablering av de regionala it-brottscentrum, RC3**

#### **Iakttagelser**

SC3 inrättades med uppgift att bland annat arbeta för att skapa enhetlighet för svensk polis inom ramen för Noas processansvar. RC3 skulle spegla de funktioner som finns på SC3 och varje enhet ska innehålla funktionerna desk, utredning av Isöb, komplexa cyberbrott (KCB) samt it-forensik och internetinhämtning<sup>12</sup>.

Enligt intervjuer har SC3:s arbete med att ge råd och stöd till etablering av RC3 utförts väl. Arbetet har skett med högt tempo och de olika RC3:s anpassningsförmåga har varierat. Trots utmaningar med att bedriva den egna verksamheten för it-forensiken har RC3 uppskattat stödet från SC3 och engagemanget som genomsyrat arbetet. NFC och it-avdelningen har genom arbetet i samverkansgrupperna och ämnesområdena bidragit med ett uppskattat stöd till RC3. För att vara i fas med etablering av RC3 har SC3 fått prioritera arbete med de processövergripande frågorna och på sådant sätt varit ett stöd till NFC:s processansvar.

När det gäller ambitionerna utifrån beslut om resursdimensionering och finansiering av etablering av RC3 har intervjuer och genomgång av olika dokument visat att arbetet med att etablera RC3 har prioriterats olika i polisregionerna. Tempot i etableringsarbetet har varierat. Det är inte alla RC3 som förbrukat de tillskjutna medlen<sup>13</sup> och det har varit oklart huruvida medlen ansetts vara öronmärkta för RC3. Enligt uppgift tillkom beslut om reviderade budgetramar med fördelning av medel för att finansiera uppbyggnad av etablering av RC3 utifrån krav från regionpolischefer. Internrevisionen har under granskningens genomförande uppfattat det som att några polisregioner ansett att de tillskjutna medlen skulle förbrukas genom sedvanlig prioritering mellan olika verksamhetsområdena.

RC3 ska under 2018-2020 etableras i samtliga polisregioner. It-forensiker tillhör organisatoriskt it-brottscentrum och är i de flesta fall placerade vid polisområdenas huvudorter. Förutsättningarna har varit olika i polisregionerna beroende på hur tillskjutna medel använts, det regionala stödet från stödprocesserna: HR avseende rekrytering, it-

<sup>12</sup> Rapport RC3-projekt 2019, A198.995/2018.

<sup>13</sup> Beslutsprotokoll 35/2018, 108/2018 A495.066.2016.

avdelningen för olika it-stöd och EA vad gäller lokaler. Lokala förutsättningar på arbetsmarknaden har också påverkat etableringen. Hur arbetet med inrättandet av RC3 styrts har också berott på hur polisregionernas it-forensiska verksamhet var organiserad innan beslutet om etablering av RC3. För de polisregioner som hade kommit längre med den it-forensiska verksamheten har det också varit lättare med anpassning till den nya RC3 organisationen.

### **Bedömning**

Beslut om inrättande av RC3 med den organisationsstruktur som etablerats på Noa fattades i juni 2018. Internrevisionens bedömning är att polisregionerna och verksamheterna inom RC3 och Noa har utifrån förutsättningar och förmåga kommit långt med etableringsarbetet. Det it-forensiska området har varit eftersatt men det har nu gjorts framsteg genom bland annat ett förbättrat samverkansarbete för it-forensik. Internrevisionen anser att SC3 arbete med de processövergripande frågorna har varit ett viktigt stöd för att få etableringsarbetet framåt.

### **Rekommendation 4.1.1**

#### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att NFC tillsammans med SC3 och regionala RC3 utvärderar och tillvaratar goda exempel vid myndighetens etablering av regionala it-brottscentrum. Med utgångspunkt från denna utvärdering bör beslut fattas avseende vidareutveckling och förvaltningen av den it-forensiska verksamheten.

Konsekvensen av om rekommendationerna inte följs är att Polismyndighetens it-forensiska arbete bedrivs ineffektivt, vilket leder till att de strategiska och operativa målen med brottsupplösning inte uppnås.

## **4.2 Resursdimensionering personal**

### **Iakttagelser**

#### **NFC**

Enligt tidigare iakttagelser i avsnitt 3 framgår att NFC:s sektion för informationsteknik inte anses vara rätt resursdimensionerad för uppdraget som processansvarig för it-forensik, ansvaret för FoU samt ärendehantering vad gäller komplexa it-forensiska undersökningarna. NFC har påtalat resursbehovet i myndighetens budgetdialog. För 2019 har de tilldelade medlen förbrukats. Fördelningen av arbetstid/resurser mellan ärendehantering och FoU uppges inte vara optimal. Det har uppgetts att det finns ett mycket stort behov av utveckling inom informationsteknik och att FoU måste prioriteras bättre. Vidare har det påpekats vikten av att myndigheten inte tappar mark internationellt då detta samarbete är viktigt för utveckling av myndighetens it-forensik och därmed en framgångsrik brottsbekämpning och upplösning.

#### **RC3**

Granskningen har visat att den it-forensiska verksamheten har utmaningar med resursättning utifrån de beslutade nationella ambitionerna. Polisregioner har genomfört olika utredningar, översyn av de egna RC3 verksamheterna samt inlämnat analyser och budgetunderlag avseende resurser. De regionala RC3 har haft olika resursnivåer baserade på det regionala behovet. Enligt uppgifter till internrevisionen har följande framkommit

vad gäller bemanning av it-forensiker.<sup>14</sup> RC3 Stockholm har ett planerat behov av 83 it-forensiker och per november 2019 finns det 43 vakanser varav 8 rekryteringar pågick. Det har uppgetts att Stockholm tappat 40 % av sin personal totalt på RC3 de senaste två åren. För RC3 Väst har det vid ingången till etableringen funnits 34 medarbetare totalt på RC3 och per december 2019 finns det 75 medarbetare, varav 40 it-forensiker. Region Bergslagen etablerade regionalt it-brottscentrum i maj 2019, då fanns 16,5 it-forensiker. Vid slutet av 2019 fanns 19,5 it-forensiker och under våren 2020 kommer det att finnas 24 it-forensiker. Region Öst har under 2018-2019 rekryterat ett tiotal it-forensiker vilket skett enligt plan. Enligt Östs beräkningar uppgår behovet av it-forensiker till 23-31 totalt.

Enligt riktlinjer för den it-forensiska verksamheten och den konsekvensanalys som genomförts avseende effekter vid införandet av riktlinjerna pågår ett arbete med att ta fram en myndighetsgemensam bild av resursbehovet. I konsekvensunderlaget redovisas en uppskattning avseende behovet av funktionen it-forensiker. Ett nyckeltal som har använts för att skatta behovet är att en it-forensiker kan stödja 3-4 brottsutredare. I myndigheten finns det idag ca 350 it-forensiker och ca 7 000 utredare. Detta innebär att 1 it-forensiker ska biträda 20 utredare. Det har skett en renodling av arbetsuppgifterna och rollerna inom it-forensiken för att it-forensiker ska kunna fokusera på it-forensisk undersökning och analys. Numera finns bland annat funktionerna internetinhämtare, Isöb-utredare och it-analytiker. Andra förändringar för att renodla är decentralisering av enklare it-forensiska uppgifter som kan utföras av handläggare samt införande av verktyg som möjliggör att utredare får tillgång till brottsutredningens digitala information och då själva kan leta och analysera bevismaterial. Trots dessa genomförda och planerade förändringar ser den it-forensiska verksamheten att det finns behov av minst en fördubbling av antalet it-forensiker inom en tvåårsperiod<sup>15</sup>.

Resursbrister har inneburit att det it-forensiska stödet inte möter den efterfrågan som finns inom utredningsverksamheten och stora balanser har byggts upp inom RC3. Det har uppgetts att det förekommer att utredare inte begär it-forensiskt stöd då de utgår ifrån att ärenden inte kommer kunna hanteras. En annan konsekvens har varit att utredare själva genomför it-forensiska undersökningar (av enklare karaktär). Då utredare många gånger inte har tillräcklig teknisk utrustning och it-forensisk kompetens, har det uppgetts att det finns risk att utredarnas undersökningar brister vad gäller rättsäkerhet.

## Bedömning

Internrevisionens bedömning är att den it-forensiska verksamheten inte har tillräckligt med personella resurser. Det är viktigt att resursdimensionering av den it-forensiska verksamheten görs och utgångspunkten är utredningsverksamhetens behov av it-forensiskt stöd.

<sup>14</sup> Uppgifterna som internrevisionen tagit del av har presenterats på olika sätt och inkommit vid olika tidpunkter till internrevisionen.

<sup>15</sup> Konsekvensanalys avseende införande av riktlinjer för it-forensisk verksamhet, dat 2019-11-12.

### **Rekommendation 4.2.1**

#### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att processägare för it-forensik tar fram ett planeringsunderlag för verksamhetsansvarigas resursdimensionering för den it-forensiska verksamheten vid NFC, Noa och RC3.

Konsekvensen av om rekommendationerna inte följs är att Polismyndighetens it-forensiska arbete bedrivs ineffektivt, vilket leder till att de strategiska och operativa målen med brottsupplösning inte uppnås.

## **4.3 Verksamhetsansvaret hos NFC och RC3<sup>16</sup>**

### **4.3.1 Förmågor**

#### **Iakttagelser**

När det gäller vilka typer av undersökningar och analyser (typ av tjänster) som utförs hos RC3 och NFC har framkommit att dessa inte alltid är kända inom utredningsverksamheten. Det har lyfts under intervjuerna att RC3 och NFC behöver förmedla vilka tjänster och förmågor som finns inom den it-forensiska verksamheten. Avseende förmågor handlar det både om vilken kompetens som finns hos it-forensiker men även vad som är möjligt att utföras rent tekniskt. Ett starkt personberoende har uppgetts finnas och då särskilt för nyutvecklad och avancerad it-teknik.

### **4.3.2 Dialogen UL och it-forensik**

I riktlinjer för den forensiska verksamheten framgår i beskrivningen av den it-forensiska processen att en dialog om begäran av it-forensisk undersökning kan ske redan vid brottsmisstanke. En löpande dialog ska sedan ske under förspaning, förundersökning och vid leverans av ett undersökningsprotokoll/rapport. Inledande aktiviteter i den it-forensiska processen ska enligt riktlinjerna bestå av identifiering och planering där arbetet omfattar förberedelse inför en utredning där it-forensiska undersökningar kan komma att genomföras. Målsättningen är att identifiera vilken information som eftersöks i ärendet och var denna information kan återfinnas. Denna process bör göras i nära samverkan med övrig planering inom utredningsprocessen. I riktlinjerna framgår även att aktiviteten *säkra* omfattar omhändertagande av beslag med målsättning att så stor del som möjligt av lagrad information bevaras för fortsatt undersökning. Detta genomförs ofta i samband med platsundersökning eller vid en husrannsakan.<sup>17</sup>

#### **Iakttagelser**

I intervjuerna har det framförts behov av att it-forensiker involveras tidigt i utredningar och att det sedan säkerställs en kontinuerlig dialog mellan utredare och it-forensiker. På grund av främst begränsade personella och tekniska resurser finns det stora ärendebalanser i den it-forensiska verksamheten. Dialogen mellan UL och it-forensik såsom den beskrivs i riktlinjerna sker i praktiken i alltför begränsad omfattning. Det har framkommit att dialogen mestadels handlar om beställning av it-forensiska åtgärder från utredare och it-forensikernas redovisning av genomförda undersökningar.

<sup>16</sup> Framgår det inte att iakttagelser avser specifikt NFC eller RC3, avser texten båda aktörer. Granskningen har inte omfattat it-forensisk verksamhet vid SC3, se avsnitt 2.4.

<sup>17</sup> PM 2020:18.

Granskningen visar att det för närvarande inte finns något systematiskt sätt för chefer och medarbetare att samverka och utbyta kunskap och erfarenheter. Detta gäller internt inom den egna polisregionen men även mellan andra polisregioner samt Noa och NFC. Det har uppgetts att det saknas ändamålsenliga tekniska möjligheter att dela information snabbt och enkelt, målgruppsinriktad eller till större grupperingar. Verktyg till stöd för detta har kravställts i samband med arbetet med den nationella it-forensiska miljön.

### 4.3.3 *Beställningar från utredningsverksamheten*

#### **Iakttagelser**

Intervjuer med NFC, RC3 och utredare visar på behov av att beställningsförfarandet förbättras och förenklas. Beställningar hanteras inte alltid genom användning av tillgängliga it-verktyg. Beställningar kan inkomma genom telefonsamtal och mail eller genom att endast beslag med enkla lappar inkommer till RC3. Beställningsblanketten har inga standardiserade texter för beställning vilket medför att beställningarna blir otydliga, innehåller ej de uppgifter som mottagaren behöver och inte är tillräckligt detaljerade. Beställningskoder är otillräckliga och inte tillräckligt anpassade till it-forensiska behov. Beställningen som sker i TekPro är uppbyggd utifrån generell forensik. Vidare saknas det koppling till Durtvå och NFC:s Forum.

It-forensiker upplever att utredningspersonal generellt saknar kunskap om vad som ska beställas och vilka undersökningar som kan genomföras. För en beställning med en cd-skiva kan det t.ex. enbart anges "hjälp". Det förekommer att bilder med timtal av material skickas in utan angivelse av att det endast är 30 sek som ska undersökas. Av en annan beställning framgår det "all kommunikation (samtalslistor, SMS, Chatt, MMS) från det senaste halvåret" vilket leder till att undersökningsprotokollet blir hundratals sidor. Ett annat exempel är beställningen "eftersök adekvat data". För en mobilextraktion kan syftet med beställningar anges som "sedvanlig tömning av mobiltelefon för utredningen". Internrevisionen har tagit del av ett antal begäranden/beställningar från TekPro där informationen från intervjuerna vad gäller den bristande kvalitén i beställningar bekräftas. Utredningsverksamheten har uppgett att de saknar tillräckligt metodstöd vad gäller it-forensik i de inledande åtgärderna i utredningar. Det har uppgetts att it-forensik inte är tillräckligt beskriven i PNU.

### 4.3.4 *Ärendehantering inom RC3*

#### **Iakttagelser**

Utredningsverksamheten har höga balanser med ärenden som behöver it-forensiskt stöd och ärendebalanserna är likaså höga hos RC3. Prioritering i utredningsverksamheten sker utifrån frihetsberövade, barn- och ungdomsärenden och utifrån straffvärde. Detta gör att grova brott och Isöb är de som prioriteras högst. På grund av bristande resurser och förmåga i den it-forensiska verksamheten får mängdsbrottsärenden knappast något it-forensiskt stöd. Isöb och grova brott får inte heller tillräckligt med stöd. Processägare för den it-forensiska verksamheten har för RC3 inte fastställt ett systematiskt sätt att hantera ärenden enhetligt i myndigheten. För att hantera ärendebalansen utifrån befintliga resurser och tekniskt stöd har det påtalats behov av ett systematiskt sätt att prioritera ärenden och ett förändrat arbetssätt. Det uppges finnas behov av att samordna och

fördela ärenden inom de olika RC3 utifrån kompetens och tillgängliga resurser och inte endast utifrån utredningsenhetens geografiska ort.

Enligt riktlinjer för den it-forensiska verksamheten finns det ett antal aktiviteter inom den it-forensiska processen: identifiering och planering, säkra, extrahera, analys, värdera, redovisa. Enligt intervjuer är mobilextraktion/tömning den mest förekommande undersökningstypen inom RC3. Det har framförts i intervjuerna att dessa undersökningar av mobiltelefoner inte utförs fullständigt. Aktiviteten *extrahera* består av olika delmoment: preparering av enhet, extrahera/avbilda data och verifiera extraherad data. Data som extraherats från en elektronisk enhet måste också ofta tolkas, dvs. konverteras till information som ett system, verktyg eller en människa kan förstå. Detta kan innebära att dekryptera information, strukturera information, återskapa information etc. Delprocessen *analysera* innebär att identifiera och samla in information som är relevanta utifrån en frågeställning i aktuell brottsutredning. Med detta menas både lagrad information och funktionsbeskrivning av elektronisk enhet eller applikation. I delprocessen *analysera* ingår också att svara på tekniska frågeställningar kopplat till den information som behandlas i undersökningen. I intervjuerna har framkommit att majoriteten av extraktionerna endast består av tömning av enheter. Utredarna får inte tillräckligt stöd med att tolka och analysera informationen.

#### **4.3.5**      *Leveranserna till utredningsverksamheten*

##### **Iakttagelser**

Det har uppgetts att på grund av balanser, otillräcklig förmåga hos it-forensiker och utredare, avsaknad eller ej tillräckligt utvecklade it-stöd, etc. finns det brister i de it-forensiska undersökningarna som utförs av RC3. Detta avser i första hand kvalitet men innebär också att undersökningar inte anses vara fullständiga. Informationen i avspeglningar som ofta görs för mobilextraktioner är svårtolkad av utredningsverksamheten då den ofta är teknisk och inte analyserad. Metodstöd saknas, alternativt är inte tillräckligt utvecklat vad gäller handböcker, arbetsrutiner, instruktioner för it-forensiker. It-stöden ger inte ett tillräckligt stöd för de undersökningar som behöver genomföras. Det pågår ett arbete där undersökningsprotokollen ska ses över när det gäller vilken typ av redovisning och innehållet i protokollen.

#### **4.3.6**      *Bedömning samtliga avsnitt under 4.3*

Internrevisionen anser att it-forensikens arbete försvåras av att det inte finns kategorisering av tjänster/förmågor. De förmågor som finns inom RC3 och NFC behöver innehålla de typer av undersökningar som kan tillhandahållas. Typundersökningar bör beskrivas utifrån vilka förmågor som finns, personell kompetens och teknik. Det är viktigt att tjänsterna är enhetligt utformade i myndigheten och att de kommuniceras och förankras i utredningsverksamheten.

Internrevisionen anser att dialogen mellan UL och it-forensik behöver utvecklas och förbättras. Precis som för kriminalteknik behöver it-forensiker involveras tidigt i utredningar. Målsättning bör vara att en dialog påbörjas redan vid ett ärendets inledningskede och att dialogen pågår kontinuerligt. För ett kvalitativt och rättsäkert resultat av från det it-forensiska stödet och i utredningar är det viktigt att samverka inte endast



består av att utredningsverksamheten beställer it-forensik och att it-forensiken levererar undersökningsprotokoll.

Internrevisionen anser att det finns ett behov av en ökad insikt och förståelse för varandras verksamheter, it-forensiker och utredare. Internrevisionen anser att det behövs en struktur och forum för spridning och förankring av information, metoder, erfarenhetsutbyte, etc. Processägare för it-forensisk verksamhet bör säkerställa att kravställningen av de tekniska möjligheterna för att förbättra samverkan och kontaktytorna mellan utredare och it-forensiker följs upp.

Arbetet med utredningsverksamhetens beställningar/begäran om it-forensiskt stöd behöver förbättras. Utredningsverksamheten tillsammans med it-forensiken behöver behovsinventera utvecklings- och förbättringsbehov för beställningsförfarandet. Utredningsverksamheten behöver utbildas i hur de it-forensiska undersökningarna kan beskrivas vid beställning.

Internrevisionens bedömning är att det finns behov av att förbättra prioritering, ärendetilldelning och arbetssätt i den it-forensiska verksamhetens ärendehantering. I arbetet med att vidareutveckla och förvalta RC3 verksamheterna är det av vikt att kompetens och förmåga kartläggs och synliggörs. I detta arbete bör den it-forensiska verksamheten utforma ett enhetligt och systematiskt sätt att prioritera och fördela ärenden. De stora ärendebalanserna behöver hanteras mer systematiskt utifrån ett myndighetsperspektiv. Det finns förbättringsmöjligheter vad gäller den it-forensiska verksamhetens leveranser av undersökningsprotokoll till utredningsverksamheten. Den it-forensiska verksamheten bör tillsammans med utredningsverksamheten arbeta fram vilka förändringar som behöver genomföras för att undersökningsprotokollen ska motsvara behov och förväntningar hos utredningsverksamheten. Bland annat bör följande faktorer omfattas: ansvar och roller, ärendehantering, dialogen utredare och it-forensiker, beställningar och leveranser inom it-forensik. När det gäller undersökningsprotokollen bör processägaren säkerställa att påbörjade förändringar fullföljs, implementeras och förankras i den it-forensiska verksamheten.

#### **Rekommendation 4.3.6**

##### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att processägare för it-forensik, tillsammans med processägaren för UL, vidtar de åtgärder som krävs för att förbättra ärendehantering inom it-forensiken.

#### **Rekommendation 4.3.7**

##### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att processägare för it-forensik tar fram en struktur för dialog och samverkan mellan utredare och it-forensiker inom NFC, SC3 och RC3. Vidare bör de kravställda tekniska möjligheterna utvecklas för att stödja samverkan.

Konsekvensen av om rekommendationerna inte följs är att Polismyndighetens it-forensiska arbete bedrivs ineffektivt och bidrar inte tillräckligt till uppfyllelse av myndighetens mål med brottsbekämpning och upplärning. Detta kan medföra betydande negativa konsekvenser på ärendehantering inom it-forensiken och utredningsresultatet.

## 4.4 Informationsförvaltning, arkiv och gallring

### Iakttagelser

Vid intervjuer med RC3, NFC och RA har framkommit att det finns förbättringsmöjligheter när det gäller hur informationsförvaltning och arkivering hanteras i den it-forensiska verksamheten. Vid intervju med RA uppges det att regelverk för gallring och hantering av it-forensiska handlingar enligt Riksarkivets föreskrifter finns tillgängligt på Intrapolis, men att den it-forensiska verksamheten inte efterlever dessa i tillräcklig omfattning. Inom NFC regleras informationsförvaltning och arkiv för it-forensik i ledningssystemet för NFC. När det gäller it-forensik utanför RC3 uppges det finnas behov av förbättrad kunskap och efterlevnad. När t.ex. utredare hanterar it-forensiska beslag själva utan it-forensisk kompetens leder det generellt till att dokumentation, dumenthantering, arkivering, gallring och bevarande inte sker på rätt sätt.

Det har uppgetts finnas otydlighet kring hur RA kan stödja den it-forensiska verksamheten med hantering av it-forensiskt material samt dokumentation- och bevaringsfrågor. It-forensiken ackumulerar enorma mängder data som är svåra och kostsamma att lagra, och med stort antal irrelevanta personuppgiftsbehandlings. Gallringsfristerna är svårtillämpade särskilt när det gäller spegling av information i beslag. NFC har uppgett att det har till RA inlämnats en begäran för att harmonisera och förenkla arkiv- och gallringsreglerna för it-forensiskt material.

Inför utveckling av nationell it-forensisk miljö har RA involverats vad gäller strukturen för arkivering. NFC har beställt en informationsanalys gällande den nationella it-forensiska miljön. För it-stödet *utredning it-forensik* har SC3 beställt en informationsanalys för den utredande och it-forensiska verksamheten utifrån samtliga användares behov. RA har uppgett att det finns behov av att ta ett helhetsgrepp för arkiverings- och gallringsfrågor i den it-forensiska verksamheten.

### Bedömning

Internrevisionen anser att det finns behov av att se över hur arbetet med informationsförvaltning, arkivering och gallring av data inom den it-forensiska verksamheten, ska hanteras. NFC behöver lämna in en ny begäran till RA gällande vilka förbättringar som bör genomföras inom detta område.

#### Rekommendation 4.4.1

##### Orange – Väsentlig brist

Internrevisionen rekommenderar att processägare för it-forensik, med stöd av RA, klargör hur den it-forensiska verksamheten ska möta de interna och externa krav som finns för informationsförvaltning, arkivering och gallring.

Konsekvensen av om rekommendationen inte följs är att hantering av informationsförvaltning, arkivering och gallring i den it-forensiska verksamheten fortsätter att hanteras på ett felaktigt sätt. Detta kan leda till att betydande negativa konsekvenser för myndighetens lagringskostnader och rättsäkerheten.

## 5 It-system, it-tjänster, it-infrastruktur

Enligt arbetsordningen<sup>18</sup> har it-avdelningen verksamhetsansvar och chefen för avdelningen är processägare för att bland annat tillhandahålla it-tjänster till myndighetens olika enheter, myndighetens inköpsverksamhet inom it-området, att utveckla, förvalta och sköta drift av samtliga it-system och it-infrastruktur, att bistå avdelningarna så att dessa kan fullgöra sitt ansvar som kravställare av it-system. NFC har enligt arbetsordningen<sup>19</sup> verksamhetsansvar för att, i samverkan med ekonomiavdelningen (EA) och it-avdelningen, upphandla och utveckla forensiska it-system och register.<sup>20</sup> Enligt beslut<sup>21</sup> om samverkan mellan NFC, Noa och polisregionerna ska de olika enheterna samarbeta kring kravställning, it-infrastruktur och andra gemensamma frågor som berör it-forensisk verksamhet. Samverkan förtydligas i NFC beslut om riktlinjer för samverkansråd it-forensik.

I it-planen<sup>22</sup> för 2020 framgår att it-avdelningens målsättning är att skapa nytta för verksamheten genom en ökad utvecklingstakt med en hög kvalitet. Detta sker genom agila arbetssätt med kontinuerliga mindre leveranser, där all utveckling och drift sker i linjen. It-planen omfattar 221 huvudleveranser som knyts till de långsiktiga mål, delmål och nyckelaktiviteter som finns i Polismyndighetens strategiska verksamhetsplan. Inom utredningsverksamheten ska flödet mellan utredning och forensik utvecklas och nya förmågor för stora förundersökningar möjliggöras i Durtvå Plus. Inom områdena it-brott och it-forensik ska utvecklas ett flertal förmågor i form av verktyg och förutsättningar i den underliggande infrastrukturen, vilket krävs för nationellt samarbete.

### Iakttagelser

Den tekniska utrustning som behövs för den it-forensiska verksamheten är avancerad. Ofta krävs speciella programvaror och hårdvara med hög kapacitet. Den infrastruktur med nätverk som används måste skyddas effektivt. It-forensiken behöver ibland vara helt isolerad från annat it-stöd. Detta medför höga kostnader för infrastruktur, hårdvara och mjukvarulicenser, samt ett starkt beroende till it-avdelningen för inköp, uppbyggnad, drift och support. Vissa verktyg ska alla it-forensiker ha. Andra verktyg kan endast några ha på en viss ort. Specialverktyg finns främst hos NFC. I intervjuer har framkommit att befintlig hårdvara inte alltid har tillräcklig kapacitet för arbetet med att behandla stora filer och att köra tunga bearbetningar. Det finns därmed behov av nya datorer och servrar, samt underhåll av utrustning och nätverk. Antalet licenser har begränsats, bland annat av kostnadsskäl. I flera fall har vissa programvaror placerats hos en eller ett fåtal RC3 där it-forensiker har fått utbildning för de specifika programmen.

Att verktygen inte räcker vad gäller omfattning och kapacitet, samt att underhåll inte sker i tillräcklig omfattning har uppgetts leda till ett antal konsekvenser, bland annat försämrad effektivitet i den it-forensiska verksamheten. It-forensiken blir en flaskhals i utredningar vilket kan leda till onödigt långa handläggningstider. I intervjuer har det lyfts fram ett stort behov av en gemensam it-miljö för den it-forensiska verksamheten. I myndigheten pågår utveckling av en plattform som ska möjliggöra att filer kan delas

<sup>18</sup> PM 2019:23, 3 kap 22 §.

<sup>19</sup> Beslutsprotokoll Noa 61/2018.

<sup>20</sup> PM 2019:23, 3 kap 19 §.

<sup>21</sup> Beslutsprotokoll NFC A008.734/2018.

<sup>22</sup> PM 2020:02

och skickas mellan de olika enheterna inom den it-forensiska verksamheten. Utvecklingen har dock inte följt tidplanen. Första steget, en central lagring för pågående undersökningar, har levererats under granskningens gång.

Därtill finns ett pågående projekt med att utveckla it-stödet *utredning it-forensik*. Med detta stöd kommer utredaren och it-forensikern kunna bearbeta digital information från beslagtagna enheter i ett anpassat webb-gränssnitt. It-stödet kan frigöra tid till mer tekniskt avancerat it-forensiskt arbete för it-forensiker och förbättra samarbetet mellan utredare och it-forensiker.

Utredningsverksamhetens beställningar till det it-forensiska stödet ska ske via ärendehanteringssystemet TekPro. Systemet är egenutvecklat i myndigheten. Under intervjuerna har framförts ett sedan länge identifierat behov av att vidareutveckla systemet. Det saknas idag en integrering till polisens utredningssystem (Durtvå), vilket gör att it-forensiker riskerar att arbeta med ärenden som redan är avslutade. Det finns dessutom behov av ytterligare funktioner i TekPro, bland annat för prioriteringsarbete, ärendetilldelning och statistik för uppföljning. Därtill finns önskemål om en koppling till analysystemet Status.

I intervjuerna har framgått att it-forensikens arbete med att behovsinventera, prioritera och kravställa mot it-avdelningen inte har fungerat tillfredsställande under flera år. Beslutet 2018 om samverkan har skapat bättre förutsättningar för detta arbete. Behovsidentifiering, prioritering och kravställning vad avser it-forensik hanteras numera av ett samverkansråd. Detta råd ska samla behoven för infrastruktur, nätverk, hårdvara, mjukvara och klienter från NFC, SC3 och RC3. Samverkansarbetet är fortfarande under uppbyggnad och i intervjuerna har framkommit att de regionala behoven ännu inte hanteras tillräckligt strukturerat. Den it-forensiska verksamheten inom RC3 känner inte alltid till hur beställningar ska ske. Samtidigt har it-avdelningen framfört till samverkansrådet att beställningar fortfarande inkommer ostrukturerat från verksamheten, och att det inte alltid är tydligt om den som beställer är behörig.

Enligt de intervjuade har det gemensamma kravspecifikationsarbetet till it-avdelningen blivit något bättre men det finns fortfarande förbättringsmöjligheter. När kravspecifikationer inkommer till ansvarig för it-forensiska system hos it-avdelningen ska dessa prioriteras, och ett arbete med förvaltning och utveckling kan påbörjas. Produkterna som beställs för it-forensik är specifika och passar inte alltid in i standardmallar för servrar, nät m.m. När prioriteringar har lämnats över till drift och infrastruktur upplever representanter för samverkansrådet att it-avdelningen tappar fart. Fördröjningarna i leveranser från it-avdelningen har uppgetts vara påtagliga. Det har uppgetts föreligga ett stuprörsarbete och därmed svårigheter att samordna beställningar. It-avdelningen har saknat fasta ansvariga för drift och infrastruktur inom it-forensik och it-brott, och kompetensen inom avdelningen har enligt uppgift varierat. I intervjuer har även framkommit att it-support saknar tillräcklig kompetens för de it-forensiska systemen, vilket har fått till följd att viss support istället sker från leverantörer.

It-avdelningens uppfattning är att sedan 2015 har de behov som framförts av den it-forensiska verksamheten varit rörliga och de har förändrats väsentligen fram till idag. Det har varit ett rörligt mål som gradvis och organiskt har växt fram, men där behovsbilden alltjämt är otydlig och angreppssättet för att fastställa behoven explorativt. Detta

arbetsätt medför betydande insatser och kostnader för it-avdelningen när idéer ska testas för att senare förkastas. Arbetssättet medför stora svårigheter för it-avdelningen att kvantifiera personella och ekonomiska insatser över tid, vidare att säkerställa att personella och ekonomiska resurser kan tillgängliggöras för att tillgodose behoven.

De insatser som genomförts i infrastrukturen har varit och är omfattande. Det handlar om en helt ny nationell driftsmiljö. It-avdelningen har framfört att det i granskningen återges en ensidig bild som inte ger rättvisa till omfattningen av de personella och ekonomiska insatser som krävs för att etablera en så komplex och omfattande infrastruktur som föreligger. It-avdelningens insatser har nästan uteslutande finansierats genom it-avdelningens anslags- och låneram och endast med mycket knappa ekonomiska och tillfälliga tillskott i form av engångsmedel. De personella insatserna som fått hantera en helt ny verksamhet i it-avdelningens linjeorganisation har varit i tillägg till det ordinarie uppdraget.

### **Bedömning**

Internrevisionens bedömning är att den it-forensiska verksamheten inte har på ett ändamålsenligt sätt behovsinventerat och kravställt it-stöd. Teknisk utrustning är avgörande för att den it-forensiska verksamheten ska kunna bedrivas. I takt med den tekniska utvecklingen i samhället uppkommer hela tiden nya behov av utrustning och kapacitet. Internrevisionen bedömer att det finns behov av att komplettera och modernisera den tekniska utrustningen för it-forensik. Befintlig hårdvara har inte alltid tillräcklig kapacitet för att behandla stora filer och att köra tunga bearbetningar. En nationell it-forensisk miljö behövs för att möjliggöra att filer kan delas och skickas mellan de olika enheterna inom den it-forensiska verksamheten. Det finns därmed ett konstant behov av förbättring av hårdvara, mjukvara och infrastruktur.

Internrevisionen anser att det är viktigt att det påbörjade arbetet med att utveckla it-stödet utredning it-forensik fortskrider enligt plan så att detta möjliggör ett effektivare arbetsätt samt förbättrar samarbetet mellan utredare och it-forensiker. Det finns även vissa effektivitetsvinster om det för RC3 kan utvecklas ett arbetsätt där vissa programvaror skulle finnas på en central licensserver. Dessa programvaror kan förläggas hos en eller ett par RC3 med särskilt utbildade it-forensiker.

Internrevisionen menar att ärendehanteringssystemet TekPro behöver utvecklas med en koppling till polisens utredningssystem (Durtvå) för att it-forensiker ska kunna se vilka ärenden som redan är avslutade. I samband med denna utveckling bör systemet även kompletteras med funktioner för prioriteringsarbete, ärendetilldelning och statistik för uppföljning.

En total inventering av teknisk förmåga bör göras. Utifrån detta kan myndigheten på nationell, regional och lokal nivå utreda och fastställa vilken teknisk kapacitet som finns, bör finnas och planera för hantering av gapet. Samverkansrådet för it-forensik kan därefter arbeta gemensamt med RC3 för att effektivisera behovsinventering, prioritering och kravställningsarbetet till it-avdelningen. Enligt uppgift har it-avdelningen saknat permanent ansvariga för drift och infrastruktur inom it-forensik och it-brott, och kompetensen hos avdelningen upplevs ha varierat. Samverkansrådet bör därför till it-avdelningen framföra behov av en ökad kontinuitet i bemanning och kunskapsnivå hos

it-avdelningen. Samordningen av beställningar med it-avdelningen behöver också ses över.

It-avdelningen har under arbetet med åtgärdsinhämtningen för de lämnade rekommendationerna inkommit med synpunkter på internrevisionens beskrivning av bland annat it-avdelningens förutsättningar för it-utveckling för den it-forensiska verksamheten. De uppgifter som nu har framförts var redan kända av internrevisionen och därför ändras inte de bedömningar som har gjorts.

## Rekommendationer

### *Rekommendation 5.1*

#### **Röd – Mycket väsentlig brist**

Internrevisionen rekommenderar att processägare för it-forensik genomför en konsekvensanalys av de förseningar som föreligger för den pågående utvecklingen av it-miljöer. Om riskerna i analysen bedöms som väsentliga och att hantering inte kan ske inom processansvariges riskägarskap, bör eskalering ske till högre beslutsnivå eller flyttas till annan riskägare.

### *Rekommendation 5.2*

#### **Röd – Mycket väsentlig brist**

Internrevisionen rekommenderar att processägare för it-forensik genomför en totalinventering/kartläggning av den it-forensiska verksamhetens behov av it-stöd nationellt, regionalt och lokalt. Efter denna kartläggning bör kravställning till it-avdelningen ske utifrån en kortsiktig och långsiktig prioritering av införskaffning, förvaltning och utveckling av it-system, it-infrastruktur och it-tjänster.

It-stöd är en grundförutsättning för den it-forensiska verksamheten. Konsekvensen av om rekommendationerna inte följs är att väsentliga moment inom it-forensiken inte kan utföras. Detta kan medföra stora negativa konsekvenser för Polismyndighetens arbete när det gäller effektivitet och lagenlighet för utredningsverksamheten, vilket allvarligt kan påverka myndighetens förmåga att uppnå målen för brottsbekämpning och uppkläring.

## 6 Kompetensförsörjning och kompetensutveckling

Enligt Polismyndighetens strategi för kompetensförsörjning är målet med myndighetens kompetensförsörjning att säkerställa att det finns rätt kompetens på rätt plats vid rätt tid, till rätt kostnad, utifrån verksamhetens behov samt myndighetens uppdrag, mål och värdegrund<sup>23</sup>. I Polismyndighetens kompetensförsörjningsplan framgår att aktiviteter, som att rekrytera eller i någon form utveckla medarbetare för att säkra myndighetens kompetensförsörjning, ska föregås av ett systematiskt arbete som består av analys, planering, genomförande av aktiviteter samt uppföljning av genomförda aktiviteter för att tillse att rätt saker görs för att säkerställa myndighetens kompetensförsörjning. Arbetet ska ske

<sup>23</sup> PM 2019:29, Saknr 799.

på flera nivåer i myndigheten. På så sätt säkerställs att medarbetare rekryteras och utvecklas utifrån identifierade behov i verksamheten<sup>24</sup>.

## 6.1 Kompetens

### Iakttagelser

Den it-forensiska verksamheten är it-intensiv och it-kompetens behöver stärkas enligt vad som framkommit i intervjuer och vid genomgång av dokument. Nuvarande kompetens inom it-området för den it-forensiska verksamheten, inklusive utredningsverksamheten och den ingripande verksamheten (IGV) är mycket varierande. It-forensikens kedja startar redan i IGV och där behöver medarbetarna ha en viss it-kompetens för att kunna hantera de initiala utredningsåtgärderna avseende bevissäkring av digitala spår. I SC3 rapport<sup>25</sup> kan det utläsas att det kan finnas digitala inslag i all brottslighet, vilket innebär att förmågan att hantera digitala inslag måste finnas på alla nivåer inom polisen. Parallellt med uppbyggnaden av RC3 måste därför en successiv kompetenshöjning ske inom hela polisen. Noa har genom sitt processägarskap för processen it-relaterade brott en plan för omhändertagande av delar av kompetenshöjning genom att införa digitala utbildningar och bidra till utveckling av lämpliga it-stöd för it-forensiker, utredare och andra lämpliga personalkategorier i myndigheten. I samverkansrådet för it-forensik pågår ett arbete med att samordna planer och aktiviteter för kompetensutveckling.

Vidare har framkommit att ämnesområdet it-forensik inte finns med i grundutbildningen för poliser. Däremot kan det förekomma att ämnet tas upp utifrån intresse hos lärare och de enskilda lärosätena. It-forensik saknas som ämne i polisutbildningen vilket har bidragit till en låg kompetens inom IGV och utredningsverksamheten. Det har framförts betydelsen av att it-forensiker får en anpassad utbildning i brottsutredning.

I det pågående kompetenssäkringsarbetet i samverkansrådet för it-forensik har ett arbete bedrivits med att ta fram kompetensprofiler för den it-forensiska verksamheten. Kompetensprofiler saknas fortfarande (under tiden för denna granskning) för de it-forensiska funktionerna inom NFC och RC3 där Noa inte har processansvar. Kompetensprofiler togs fram under våren 2019 men på grund av en ny modell för detta arbete vid HR behöver materialet konverteras. Det har lämnats synpunkter kring att det är viktigt att aktiviteterna för färdigställande av arbetet med kompetensprofiler, arbetsbeskrivningar för de olika ämnesområden, framtagande av styrdokument, interna utbildningar, etc. sker i rätt ordning. Personalen inom it-forensik är attraktiv på marknaden varför det uppgetts vara avgörande med ett genomtänkt arbete med kompetensförsörjning och kompetensutveckling för att attrahera och behålla.

I intervjuerna har det uppgetts finnas behov av olika nivåer när det gäller funktionen it-forensiker. Detta har lyfts i riktlinjerna för den it-forensiska verksamheten. I konsekvensanalysen görs en indelning i fyra kompetensnivåer: *grund*, *fördjupad*, *avancerad* och *specialiserad*. Syftet med att införa fyra nivåer anges vara att dels förenkla rekrytering av oerfaren men tekniskt välutbildad personal, och dels att skapa förutsättningar för reviderad lönesättning när en it-forensiker har nått en ny kompetensnivå.

<sup>24</sup> PM 2019:28, Saknr 799.

<sup>25</sup> Rapport RC3-projektet 2018-2019, A198.995/2018.

## 6.2 Rekrytering, bemanning och lönebildning

### Iakttagelser

Det har framkommit i granskningen att det inte finns tillräckligt med utbildningssäten för it-forensisk kompetens i Sverige. Detta har lett till en hård konkurrens om kompetensen på både den privata och offentliga marknaden. Det finns därmed inte tillräckligt med kandidater på marknaden, vilket har skapat svårigheter att rekrytera. Internt inom myndigheten finns det också en konkurrens mellan polisregioner, it-avdelningen och Noa. Det är särskilt den lönepolitiska situationen för kompetensområdet som har försvårat bemanningsarbetet. Inom ramen för ett pågående kompetenssäkringsarbete för den it-forensiska verksamheten och it-brottslighet, finns ett påbörjat samarbete med lärosäten för att föra en dialog kring att utveckla och starta upp nya utbildningar med inriktning på it-forensisk området.

Den generella uppfattningen från de genomförda intervjuerna med den it-forensiska verksamheten är att Polismyndighetens löner för it-forensiker inte är marknadsmässiga jämfört med ett antal andra myndigheter samt den privata marknaden. Den it-forensiska verksamheten har framfört att myndighetens lönepolitik behöver ses över för att hitta en gemensam inriktning för att hantera den aktuella lönepolitiska situationen. Det har vidare framkommit att samverkan mellan processansvariga för it-forensik och HR-avdelningens olika enheter för rekrytering, lönebildning och kompetensenheten inte har fungerat väl. Vid beslut om etablering av RC3 saknades tillräckligt stöd från HR-avdelningen. HR-avdelningen har uppgett att polisregionerna vid behovsinventering inför RALS-arbetet inte har inkommit med tillräckligt underlag som visat behov av särskild prioritering av den it-forensiska verksamheten. Samtidigt har HR-avdelningen uppgett att det finns behov av att förbättra arbetet med genomförande av kalibreringsamtal mellan olika verksamhetsområden.

## 6.3 Interna utbildningar

I enlighet med Polismyndighetens riktlinjer för pedagogisk inriktning ska myndigheten bedriva kompetensutveckling som på ett systematiskt sätt ställer medarbetarnas befintliga kompetens i relation till såväl individens som verksamhetens behov av förnyad eller förstärkt kompetens. Ett centralt led i detta arbete är att medarbetarna i hela landet ska uppnå relevant, likvärdig och uppdaterad kompetens för sina arbetsuppgifter<sup>26</sup>.

### Iakttagelser

Granskningen visar att interna utbildningar i form av kurser och fortbildningar har utblivit de senaste två åren för ämnesområdet it-forensik. Kortare utbildningar med avseende på spetskompetens för olika undersökningsmetoder och programvaror har kunnat erbjudas via leverantörer och NFC. Det har uppgetts att det finns ett stort behov av att utredare och it-forensiker ska förstå varandras verksamheter, vilket bland annat bör ske genom utbildningsinsatser och andra kompetenshöjande åtgärder.

Av olika skäl har inventering av utbildningsbehov inte skett på ett ändamålsenligt sätt. Det har uppgetts att under 2019 införde HR nya krav vilka verksamheten inte hade hunnit anpassa sig till. Till kompetenscentrum 2 (KC2) inkom otillräckliga kravspecifikationer med ett innehåll som inte var genomarbetat då det bland annat saknades färdig-

<sup>26</sup> PM 2016:55, Saknr 750.



ställda kompetensprofiler (enligt HR:s nya krav). Enligt KC2 försvårade detta det redan svåra arbetet med att balansera ett utbildningsutbud utifrån processägarens initiala prioriteringar. Numera finns ett samverkansråd där korsvisa prioriteringar kan göras mellan olika ämnesområden men detta saknades tidigare och gjorde att kravställning inom ostrukturerat till HR. Samtidigt har det saknats lärare/instruktörer från verksamheten. KC2 har inte varit tillräckligt bemannade för att stödja det it-forensiska utbildningsbehovet. Under granskningens genomförande har samverkansrådet för it-forensik arbetat fram en kravspecifikation för utbildningar som lämnats till HR-avdelningen för vidarehantering. I myndighetens kompetensutvecklingsplan 2020 framgår att det fastställts ett antal utbildningar för det it-forensiska ämnesområdet. NFC och SC3 anser att de planerade kurserna som prioriterats av HR-avdelningen är långt ifrån tillräckliga utifrån den it-forensiska verksamhetens behov.

Under granskningens genomförande har ett regeringsuppdrag inkommit till Polismyndigheten med avseende på kompetensförsörjning och kompetensutveckling för polisens verksamhet för it-brottslighet<sup>27</sup>.

### **Bedömning avsnitt 6**

Internrevisionen bedömer att det finns förbättringsbehov när det gäller arbetet med kompetensförsörjning och kompetensutveckling för den it-forensiska verksamheten. Detta gäller även för den utredningsverksamheten som är beställare och mottagare av det it-forensiska stödet. Processägare för it-forensik bör, med stöd av HR-avdelningen och utifrån myndighetens strategi och plan för kompetensförsörjning, tillse att planering och genomförande av olika aktiviteter sker för att säkerställa rätt kompetens i den it-forensiska verksamheten. Arbetet bör ske utifrån ett definierat uppdrag för it-forensiken men även identifierat behov av it-forensiskt stöd i myndigheten.

Internrevisionens bedömning är att det finns behov av att införa de olika nivåerna för funktionen it-forensik, vilka tas upp i riktlinjerna för den it-forensiska verksamheten. Internrevisionen anser att dessa nivåer kan bidra till en förbättring för att kunna hantera frågor kring kompetensutveckling och handläggning av ärenden utifrån kompetens och tillgänglig resurs. Nivåerna kan även stödja myndigheten vid lönesättning av it-forensiker.

Processansvarig för it-forensik bör arbeta fram en plan för att attrahera och behålla medarbetare inom den it-forensiska verksamheten och i synnerhet it-forensiker. Denna plan bör omfatta rekrytering och bemanning, lönebildning inklusive arbetet med karriär och utvecklingsvägar. Arbetet med fort- och vidareutbildningsarbetet samt kommunikationsinsatser avseende att attrahera och behålla kompetenser inom it-forensik, bör också inkluderas i planen. Det är med fördel, utifrån polisens långsiktiga mål *attraktiv arbetsplats och samarbetspartner*, att kommunikationsinsatser med stöd av kommunikationsavdelningen (KA) tas fram och bedrivs aktivt gentemot utbildningssäten och andra lämpliga aktörer i syfte att attrahera kandidater.

---

<sup>27</sup>Ju2020/00378/PO.

## Rekommendationer

### *Rekommendation 6.3.1*

#### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att processägare för it-forensik vidtar åtgärder för att stödja polisregionernas RC3 och Noa/SC3 i att införa den it-forensiska verksamheten och berörd utredningsverksamhet i strategiska inriktningar och planer för kompetensförsörjning på polisregion- och avdelningsnivå. Processägarens uppföljning av processen bör särskilt inriktas på att säkerställa nationell enhetlighet.

### *Rekommendation 6.3.2*

#### **Orange – Väsentlig brist**

Internrevisionen rekommenderar att processägare för it-forensik säkerställer ett arbete med att planera, genomföra och utveckla de fort- och vidareutbildningar som är nödvändiga för den it-forensiska verksamheten och berörd utredningsverksamhet.

Konsekvensen av om rekommendationerna inte följs är att den it-forensiska verksamheten och berörd utredningsverksamhet inte har rätt kompetens, på rätt plats, till rätt kostnad utifrån verksamhetens behov, mål och uppdrag. Detta kan medföra betydande negativa konsekvenser för den granskande verksamheten och kan innebära att myndigheten inte är effektiv i arbetet med brottsbekämpning och uppklaring.

## 7 Sammanfattande bedömning av revisionsfrågorna

Internrevisionens granskning av den it-forensiska processen visar att det finns utmaningar i hur Polismyndigheten har styrt den it-forensiska verksamheten. Det är viktigt att NFC och Noa på processägarnivå arbetar nära varandra för att identifiera aktiviteter som ska genomföras för att uppfylla målen i Polismyndighetens strategiska verksamhetsplan 2020-2024. Det har saknats en övergripande styrning av området, vilket bland annat har medfört en bristfällig resursdimensionering av de it-forensiska behoven. Övergripande riktlinjer har nu tagits fram där it-forensisk definieras och beskrivs. It-forensik, som är ett stöd i utredningsverksamheten, har inte verkat som en integrerad del av utredningsverksamheten. Vidare har processansvaret och samverkan mellan aktörerna som arbetar med it-forensik inte fungerat väl. Dock är internrevisionens bedömning att överenskommelsen om samverkan har lett till ett förbättrat samarbetsklimat. Den bristande styrningen har lett till att samverkan med stödverksamheterna IT och HR inte fungerat väl.

De övergripande frågorna i processansvaret har varit eftersatta, vilket har resulterat i att verksamheten inte maktat med att prioritera forskning och utveckling, metodutveckling, framtagande av styrdokument samt att arbeta fram ett enhetligt och systematiskt arbetsätt. Ärendehantering har prioriterats framför processansvaret men likväl har utredningsverksamheten inte fått it-forensiskt stöd på en acceptabel nivå. Den it-forensiska verksamheten har stora balanser och de it-forensiska undersökningarna som utförs har inte ansetts vara fullständiga vad gäller kvalitet. Internrevisionen anser att det finns risk

att informationsförvaltning, arkivering och gallring av data inom den it-forensiska verksamheten inte följer regelverket.

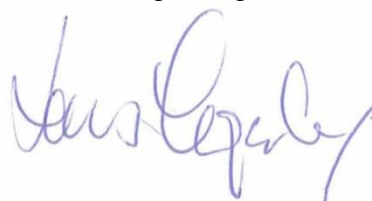
Internrevisionens bedömer att behovet av it-stöd för it-forensik, både för it-forensiker och utredare, inte har tillgodosetts tillräckligt. Den it-forensiska verksamheten är i hög grad beroende av it-stöd, vilket gör att myndigheten behöver fastställa vilken teknisk kapacitet som ska finnas för att möta efterfrågan i utredningsverksamheten.

Kompetensförsörjnings- och kompetensutvecklingsområdet avseende den it-forensiska verksamheten behöver hanteras på ett mer systematiskt sätt och utifrån myndighetens beslutade strategi och plan. Den it-forensiska verksamheten är it-intensiv och it-kompetens behöver förstärkas. Avsaknad av it-forensik som ämne vid den polisiära grundutbildningen har medfört bristande grundkompetens vad gäller it-forensik i kärnverksamheten. Det är av vikt att it-forensiker får en anpassad utbildning i brottsutredning. Arbetet med fort- och vidareutbildningar för ämnesområdet it-forensik har varit eftersatta. Kompetensförsörjning av den it-forensiska verksamheten är en av de avgörande aspekterna för att polisen ska lyckas med en framgångsrik it-forensisk verksamhet. Interna utbildningar måste prioriteras för att hantera skillnader i kompetens hos befintlig personal men även för att möjliggöra kvalitativ internrekrytering. Det saknas en tillräcklig nivå på kandidater med it-forensisk kompetens på marknaden, både den privata och offentliga, vilket gör att polisen har en hård konkurrens om kandidater. Polismyndigheten behöver samverka bättre med utbildningsäten för att ta fram nya utbildningar. Myndigheten behöver ta fram en plan för ett arbete att attrahera och behålla medarbetare inom den it-forensiska verksamheten.

Winfred Nionzima



Lars Agerberg





Datum  
2020-09-28

Beslutsprotokoll  
RPC 138/2020

Diariernr, ärende  
A482.094/2019

Saknr  
977

Beslutande Rikspolischefen Anders Thornberg	Föredragande Verksamhetsutvecklaren Johan Gunnarsson
Övriga som deltagit i den slutliga handläggningen Avdelningschefen Helena Trolläng Avdelningschefen Henrik Dider Avdelningschefen Gunilla Hedwall Avdelningschefen Martin Valfridsson Internrevisionschefen Stina N Kristiansson	
Ärende Beslut med anledning av internrevisionens granskning av den it-forensiska verksamheten	
Beslut Internrevisionen har granskat Polismyndighetens it-forensiska verksamhet. Med anledning av detta beslutar Polismyndigheten följande:  <b>Åtgärder med anledning av rekommendation 3.1.1</b> Nationellt forensiskt centrum (NFC) ska säkerställa kompetens för att stärka sin förmåga inom samordning av arbetet rörande processansvaret för it-forensisk verksamhet samt tydliggöra resursbehovet så att processansvaret bedrivs och fullföljs i enlighet med arbetsordningen och NFC:s tilldelade ansvar enligt riktlinjerna för it-forensik. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2020.  <b>Åtgärder med anledning av rekommendation 3.1.2</b> NFC ska ta fram en modell för löpande utvärdering av samverkan mellan NFC, nationellt it-brottscentrum och regionala it-brottscentrum. Arbetet ska genomföras i samverkan med nationella operativa avdelningen (Noa) och polisregionerna. NFC ska även utvärdera samarbetet med övriga aktörer. Arbetet ska genomföras i samverkan med respektive aktör. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2020.  <b>Åtgärder med anledning av rekommendation 3.2.1</b> NFC ska i samråd med nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum kartlägga behovet av styrdokument och metodstöd för den it-forensiska processen och ta fram en handlingsplan för framtagande och implementering. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2020.  <b>Åtgärder med anledning av rekommendation 4.1.1</b> NFC ska i samråd med nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum ta fram en strategi för att vidareutveckla de regionala it-brottscentrumen i enlighet med Polismyndighetens strategi 2024. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2020.	

**Åtgärder med anledning av rekommendation 4.2.1**

NFC ska i samråd med nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum ta fram ett planeringsunderlag för resursdimensioneringen för den it-forensiska verksamheten vid NFC, nationellt it-brottscentrum och de regionala it-brottscentrumen. Den ska innehålla nyckeltal för resursfördelning och nivå. Framtaget underlag ska utgå från ett förankrat behov inom utredningsverksamheten. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2020.

**Åtgärder med anledning av rekommendation 4.3.6**

NFC ska i samråd med processägaren för huvudprocessen utredning och lagföring vidta de åtgärder som krävs för att förbättra ärendehantering inom it-forensiken. Arbetet ska innehålla kravställning av it-system. Ansvarig för åtgärdens genomförande är chefen för NFC. Kravställningen av it-system ska vara genomförd senast 31 december 2020 och övriga åtgärder ska vara implementerade senast 31 december 2024.

**Åtgärder med anledning av rekommendation 4.3.7**

NFC ska i samråd med berörda parter ta fram en struktur för dialog och samverkan mellan utredare och it-forensiker inom NFC, nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum där det inte redan existerar välfungerande strukturer. NFC ska också stödja regionerna att utveckla regionala eller regionsövergripande forum. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 30 juni 2021.

**Åtgärder med anledning av rekommendation 4.4.1**

NFC ska i samråd med rättsavdelningen klargöra hur den it-forensiska verksamhet ska möta de interna och externa krav som finns för informationsförvaltning, arkivering och gallring. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2021.

**Åtgärder med anledning av rekommendation 5.1**

NFC ska i samråd med it-avdelningen, nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum ta fram en konsekvensanalys av hur förseningar i utvecklingen av it-miljöer påverkar utredningsverksamheten inom it-forensik. Konsekvensanalysen ska omfatta

- handläggningstider
- samarbetsmöjligheter (mellan it-forensiker och med utredare, regionalt och nationellt)
- nya förmågor
- ekonomiska aspekter.

Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2020.

**Åtgärder med anledning av rekommendation 5.2**

NFC ska i samråd med it-avdelningen, nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum sammanställa kravställningen av it-stöd för den it-forensiska verksamheten. Sammanställningen ska omfatta

- inköp
- klienter

- programvaror
- it-miljö
- lagring/arkivering
- utveckling
- förvaltning.

Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2020.

#### **Åtgärder med anledning av rekommendation 6.3.1**

NFC ska i samråd med HR-avdelningen, nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum stödja polisregioner och avdelningar att föra in den it-forensiska verksamheten och berörd utredningsverksamhet i strategiska inriktningar och planer för kompetensförsörjning. Detta ska baseras på kompetensprofiler för respektive funktion. Detta ska även omfatta vilka kunskapskrav som Polismyndigheten ställer på den som anställs i myndigheten samt säkerställa karriär och utvecklingsvägar inom ramen för it-forensiken. Dessa ska utgå från kompetensnivåerna enligt Polismyndighetens riktlinjer för it-forensisk verksamhet (PM 2020:18). Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2021.

#### **Åtgärder med anledning av rekommendation 6.3.2**

NFC ska bistå i regeringsuppdraget till Polismyndigheten rörande kompetensförsörjning och kompetensutveckling avseende bekämpning av it-relaterad brottslighet. Det omfattar kompetenshöjning i hela kedjan från polisutbildningen till myndighetens specialistkompetens. NFC ska också i samråd med HR-avdelningen, nationellt it-brottscentrum och polisregionernas regionala it-brottscentrum vidareutveckla kompetensutvecklingsplanen för de kompetensnivåer som är definierade i Polismyndighetens riktlinjer för it-forensisk verksamheten. Ansvarig för åtgärdens genomförande är chefen för NFC och arbetet ska vara genomfört senast 31 december 2021.

HR-avdelningen ska i samråd med NFC fastställa gången i kravställan avseende kompetensutvecklingsinsatser. HR-avdelningen ska säkerställa den egna förmågan att tillräckligt möta verksamhetsstyrd kravställan. HR-avdelningen ska också prioritera arbetet med kompetensprofiler för it-forensik. Ansvarig för åtgärdens genomförande är chefen för HR-avdelningen och arbetet ska vara genomfört senast 31 december 2021.

Med undantag från gällande rutiner har chefen för NFC vidimerat detta beslut i särskild ordning.

Kostnad

Finansiering

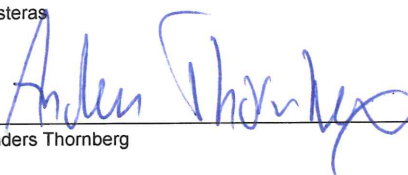
Inom budget

Vid protokollet



Johan Gunnarsson

Justeras



Anders Thornberg

2020-09-28

A482.094/2019

Sändlista

Samtliga avdelningar och polisregioner

Kopia till

Arbetsstagarorganisationerna  
Skyddsorganisationen