

Styrelsen för Nacka vatten och avfall AB

## Granskning av IT-säkerhet

### Förslag till beslut

Styrelsen föreslås besluta att:

- uppdra åt VD att inkomma med åtgärdsplan och tidplan enligt rapporten till den 15 november
- rapportera in åtgärdsplanen och tidplanen till lekmanrevisionen

Mats Rostö  
Verkställande direktör

### Ärendet

EY har på uppdrag av Nacka kommuns förtroendevalda revisorer genomfört en granskning av hur de kommunalägda bolagen arbetar med IT-säkerhet. Granskningens syfte har varit att ge en övergripande nulägesbild av huruvida Nacka kommuns Kommunstyrelse och bolagens ledningar har tillsett att arbetet med IT-säkerhet bedrivs ändamålsenligt och om det finns tillräcklig styrning och intern kontroll avseende skydd mot intrång i bolagens IT-system.

Granskningen fick i uppdrag att undersöka åtta revisionsfrågor enskilt för bolagen. För att få en något bredare bild av nuläget utgick granskningen även utifrån delar av ISO27001-standarden. Vad gäller bedömningarna för respektive fråga noteras sammanfattningsvis vilka delar som medför brister som i de flesta fall är små eller redan håller på att åtgärdas samt del som skyndsamt bör åtgärdas.

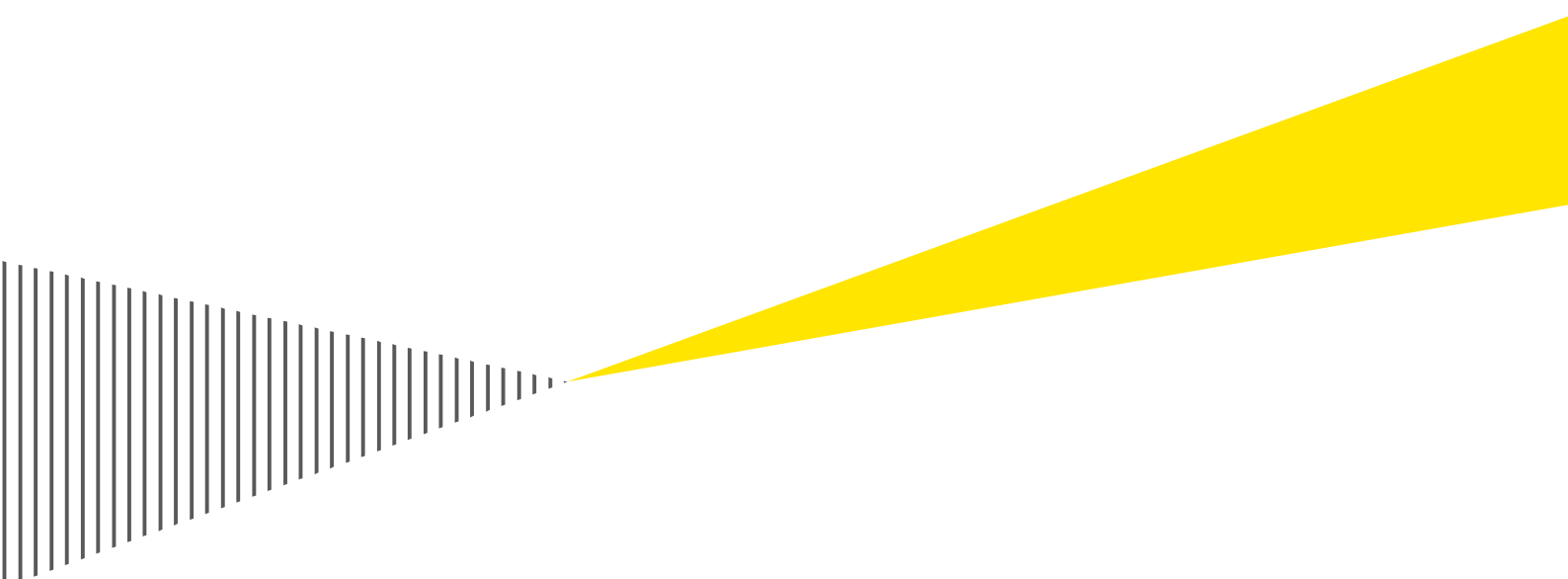
Utifrån granskningsresultatet rekommenderas bolaget att vidta åtgärder för att stärka den interna kontrollen.

**Bilagor:** Granskning av IT-säkerhet i de kommunalägda bolagen Nacka vatten och avfall och Nacka Energi AB

# Nacka kommun

Granskning av IT-säkerhet i de kommunalägda bolagen  
Nacka vatten och avfall AB och Nacka Energi AB

Augusti 2019



## Sammanfattande bedömning

EY har på uppdrag av Nacka kommuns förtroendevalda revisorer genomfört en granskning av hur de kommunalägda bolagen Nacka vatten och avfall AB och Nacka Energi AB arbetar med IT-säkerhet. Granskningens syfte har varit att ge en övergripande nulägesbild av huruvida Nacka kommuns Kommunstyrelse och bolagens ledningar har tillsett att arbetet med IT-säkerhet bedrivs ändamålsenligt och om det finns tillräcklig styrning och intern kontroll avseende skydd mot intrång i bolagens IT-system.

Granskningen fick i uppdrag att undersöka åtta revisionsfrågor enskilt för Nacka vatten och avfall AB (NVOA) och Nacka Energi AB (NEAB). För att få en något bredare bild av nuläget utgick granskningen även utifrån delar av ISO27001-standarden.

Vad gäller bedömningarna för respektive fråga noteras sammanfattningsvis att de gröna inte behöver föranleda någon åtgärd, de gula medför brister som i de flesta fall är små eller redan håller på att åtgärdas, och de röda är sådana som skyndsamt bör åtgärdas.

För gula och röda noteringar listas även förslag på åtgärder. Den enda röda noteringen i denna granskning berör fråga 7 för Nacka Vatten och Avfall. Se vidare i rapporten för detaljer.

Revisionsfrågorna listas nedan med följande sammanfattande bedömningar:

Revisionsfråga	NVOA	NEAB
1. Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policies?		
2. Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?		
3. Har bolagen ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?		
4. Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång? Vilka incidenter har inträffat och hur har styrelsen fått kännedom om dessa?		
5. Har tester genomförts avseende intrång i systemen?		
6. Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag samt hur ser kopplingen ut till bolagens interna kontroll?		
7. Hur säkerställer styrelsen att den interna kontrollen är tillräcklig och fortlöpande aktuell?		
8. Hur säkerställs att tillräcklig intern kontroll finns hos upphandlade företag som sköter driften av IT?		

### Färgkoder

Väsentliga brister har identifierats.

Brister har identifierats.

Inga väsentliga brister har identifierats.

## *Sammanfattande kommentarer kring respektive område*

### *1 Styrning av skydd mot intrång*

Båda bolag har inlett arbetet med övergripande styrning och intern kontroll, skapat styrdokument i form av relevanta IT-policyer som beskriver aktiviteter som ökar informationssäkerheten och inlett arbetet med att utveckla ett ledningssystem för informationssäkerhet (LIS) och/eller med att följa NIS-direktivet. Det saknas dock processer för kommunikation och uppdatering av policyer och tydliga krav på metodik, genomförande, uppföljning och kontroll av informationssäkerhetsaktiviteter. Brister har noterats vad gäller de beslutade dokumentens koppling till kommunkoncernens IT-policyer.

NEAB:s informationssäkerhetspolicy och ev. övriga styrdokument behöver kompletteras med styrelsens ansvar för intern kontroll över informationssäkerhet.

### *2 Riskanalyser avseende IT-säkerhet, och 5 - tester avseende intrång i systemen*

På NVOA finns ett pågående initiativ där man dokumenterar informationshanteringsprocesser och detta kan vara utgångspunkt till det framtida riskarbetet. För "sina egna" system har NVOA genomfört informationsklassningar, risk- och sårbarhetsanalyser och tekniska analyser (penetrationstester) med prioriterade handlingsplaner som resultat. NVOA söker samarbete med kommunen som står som ägare av flera system som används i verksamheten.

I intervjuerna med NEAB anges att risker analyseras. NEAB genomför riskanalyser enligt Svk:s (Svenska Kraftnät) regler och enligt El:s (Energimarknadsinspektionen) instruktioner.

### *3 Skydd för databaser och system*

Risken att obehöriga skaffar sig tillgång till databaser och system minskas i båda bolagen genom segmentering och segregering av nätverk. Brandväggarnas konfigurering går regelbundet igenom per automatik.

En tidigare brist hos NVOA, där ett system låg på fel nätverk, åtgärdades. Däremot finns i dagsläget inga konkretiserade åtgärdsplaner att begränsa de lokala domänadministrationsrättigheter som alla anställda har på sina enheter och som t.ex. ökar risken att skadlig mjukvara installeras. NVOA har kommunicerat vikten av säkerhet och enkla skyddsåtgärder till anställda som arbetar vid pumpstationer som är en kritisk del av bolagets infrastruktur och verksamhet.

NEAB:s årliga genomgångar av brandväggkonfigureringen dokumenteras inte. Processen för genomgång kommer att dokumenteras vid nästa tillfälle. Skyddet mot intrång bygger dock på en kombination av fysisk säkerhet, nätverkssegmentering, nätverkssegregering, ändamålsenliga behörighetsstrukturer och behörighetsprocesser som bör säkerställa skydd för databaser och system. NEAB har kommit långt i arbetet med dokumenterade behörighetsrutiner.

### *4 Incidenthantering*

Båda bolag saknar vid granskningstillfället formell, dokumenterad IT-incidenthanteringsprocess, även om en sådan omnämns i informationssäkerhetspolicyerna. Det finns dock korta kommunikationsvägar inom bolagen som påskyndar lösningar utan dokumenterade processer.

NVOA har etablerat en kris- och beredskapsgrupp för verksamhetsincidenter såsom verktyg för att informera medborgare som drabbas vid en incident. De har även en incidentprocess kopplat till NIS och informationssäkerhetslagen för samhällsviktig verksamhet. Verktyget används även för personuppgiftsincidenter och det finns en dokumenterad personuppgiftsincidentprocess. Det saknas kommunikationsriktlinjer mellan IT-driftsleverantören, kommunen och NVOA för IT-incidenter som rör bolaget.

NEAB upprätthåller en kultur som värdesätter rapportering till ledningen och samarbete i incidentfall. Hittills har NEAB använt sig av informella arbetssätt för att hantera de incidenter som har inträffat. Utöver detta har resan till mer standardiserade incidentprocesser påbörjats i form av en gemensam utbildning och inom NIS-projektet. NEAB har en dokumenterad personuppgiftsincidenthanteringsprocess med tillhörande roller och aktiviteter. Vid övriga incidenter följer NEAB MSB:s "Vägledning för rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen" till MSB.

## *6 Ändamålsenlig organisation*

Inom båda bolag är informationssäkerhet ett prioriterat område och policyer sätter upp en principiellt ändamålsenlig organisation. I båda bolag finns behov att genomföra periodiska utbildningar med fokus på informationssäkerhet, även vid nyanställning.

NVOA:s IT-organisation växer och ett nytt säkerhetsråd har en helhetsyn på säkerhetsfrågor, men organisationen upplever att det finns brist på personal, särskilt i sammanhanget med den löpande utvecklingen av ledningssystemet. Kunskaps- och informationsutbytet med kommunen är informellt och personberoende.

De som arbetar med informationssäkerhet hos NEAB upplever att det finns tillräckligt med resurser. Samarbetet med NEAB:s (mjukvaru-)leverantörer och övriga samarbetspartners fungerar bra, men det finns inget strukturerat kunskaps- och informationsutbyte med kommunen.

## *7 Intern kontroll*

I båda bolag saknas en tydlig koppling av informationssäkerhetsarbetet till internkontrollfunktionen som historiskt inte har tittat på informationssäkerhetsfrågor. Det saknas dokumenterade informationskrav som verksamhetens, vd:ns och kontrollfunktionens rapportering till styrelsen bör utgå ifrån, vilket kan leda till att rapporteringen inte sker med regelbundenhet/frekvens.

För NVOA saknas tydliga krav på kontrollmiljön, kontrollaktiviteter och rapporteringen från styrelsens sida. Se rekommendationer i sektion 2.1.7.

Policyer beskriver hos NEAB ansvar och roller på ett övergripande sätt. De kompletteras med befattningsbeskrivningarna. Det saknas information om styrelsens ansvar.

Rapporteringsvägar är satta utefter organisationsstrukturen.

Vid den årliga bokslutsrevisionen har man i NEAB:s fall tidigare granskat processerna för behörigheter och säkerhetskopior.

## *8 Intern kontroll hos upphandlade företag*

NVOA:s IT-drift sköts huvudsakligen av leverantören Basefarm och täcks av ett kontrakt mellan leverantören och kommunen. Bolagets ansvar att kontrollera Basefarm begränsas mestadels till de system som är verksamhetsspecifika, till exempel skadesystemet. Här ställer NVOA några krav, t.ex. på aktivitetsloggning, men organisationen saknar detaljerad kunskap om driftavtalets innehåll och därmed om omfattningen av sitt kontrollansvar.

Driften av NEAB:s nuvarande IT-miljö sköts internt. Delar av underhållet sköts med stöd av konsulter. I övrigt finns det etablerade supportavtal för de flesta leverantörer. Det finns en upphandlingspolicy och en separat checklista med säkerhetskrav. Den befintliga checklistan med säkerhetskrav är dock inte refererad som bilaga till policyn. I upphandlingsprocessen har IT-organisationen rollen som rådgivare och kravställare. Inga uppföljningar av leverantörer krävs enligt policy. I praktiken ställer NEAB dock krav på informationssäkerhet och gör uppföljningar i officiella forum.

# Innehållsförteckning

<b>1. Inledning</b> .....	<b>6</b>
1.1. Bakgrund .....	6
1.2. Syfte och revisionsfrågor.....	6
1.3. Avgränsningar.....	6
1.4. Metod och genomförande .....	6
<b>2. Bedömning avseende svar på revisionsfrågor</b> .....	<b>8</b>
2.1. Nacka vatten och avfall AB (NVOA).....	8
2.1.1. Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policyers?.....	8
2.1.2. Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?.....	9
2.1.3. Har bolaget ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada? .....	10
2.1.4. Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång? Vilka incidenter har inträffat och hur har styrelsen fått kännedom om dessa?.....	12
2.1.5. Har tester genomförts avseende intrång i systemen?.....	13
2.1.6. Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag samt hur ser kopplingen ut till bolagens interna kontroll? .....	13
2.1.7. Hur säkerställer styrelsen att den interna kontrollen är tillräcklig och fortlöpande aktuell? .....	15
2.1.8. Hur säkerställs att tillräcklig intern kontroll finns hos upphandlade företag som sköter driften av IT?.....	16
2.2. Nacka Energi AB (NEAB).....	18
2.2.1. Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policyers?.....	18
2.2.2. Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?.....	19
2.2.3. Har bolaget ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada? .....	20
2.2.4. Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång? Vilka incidenter har inträffat och hur har styrelsen fått kännedom om dessa?.....	21
2.2.5. Har tester genomförts avseende intrång i systemen?.....	22
2.2.6. Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag samt hur ser kopplingen ut till bolagens interna kontroll? .....	23
2.2.7. Hur säkerställer styrelsen att den interna kontrollen är tillräcklig och fortlöpande aktuell? .....	24
2.2.8. Hur säkerställs att tillräcklig intern kontroll finns hos upphandlade företag som sköter driften av IT?.....	25
<b>3. Bilaga: Källförteckning</b> .....	<b>27</b>

## 1. Inledning

### 1.1. Bakgrund

I takt med att både privata och offentliga verksamheter, såsom Nacka kommun och dess kommunalägda bolag, blir allt mer beroende av dagligt stöd från IT-system får hanteringen av risker inom IT-området allt större betydelse. För att på ett adekvat sätt hantera IT-relaterade risker och etablera god IT-säkerhet är det viktigt att förstå olika hotbilder, bedöma sannolikheter för att utsättas för skada samt balansera kostnader av skyddsmedel mot värdet av det man försöker skydda. Effektiv och framgångsrik IT-riskhantering bör således byggas på ett helhetstänk med tydliga styrningsdirektiv för att uppnå godtagbar intern kontroll avseende skydd mot intrång i IT-system.

Med bakgrund i ovan genomförde EY på uppdrag av Nacka kommuns förtroendevalda revisorer under maj och juni 2019 en granskning av hur de kommunalägda bolagen Nacka vatten och avfall AB och Nacka Energi AB arbetar med IT-säkerhet.

### 1.2. Syfte och revisionsfrågor

Syftet med granskningen var att ge en övergripande nulägesbild av huruvida Nacka vatten och avfall AB och Nacka Energi AB bedriver ett ändamålsenligt arbete med IT-säkerhet och om det finns tillräcklig styrning och intern kontroll avseende skydd mot intrång i bolagens IT-system. Granskningen syftar att ge svar på åtta revisionsfrågor:

- 1) Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policies?
- 2) Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?
- 3) Har bolagen ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?
- 4) Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång? Vilka incidenter har inträffat och hur har styrelsen fått kännedom om dessa?
- 5) Har tester genomförts avseende intrång i systemen?
- 6) Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag samt hur ser kopplingen ut till bolagens interna kontroll?
- 7) Hur säkerställer styrelsen att den interna kontrollen är tillräcklig och fortlöpande aktuell?
- 8) Hur säkerställs att tillräcklig intern kontroll finns hos upphandlade företag som sköter driften av IT?

### 1.3. Avgränsningar

De observationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom inspektion av erhållen dokumentation, såsom t.ex. styrdokument, riktlinjer och planer. Granskningen är begränsad till Nacka kommuns kommunala bolag Nacka vatten och avfall AB och Nacka Energi AB. Ingen granskning har skett av IT-säkerhetsarbetet på Nacka kommun som helhet och kommunens nämnder och förvaltningar är således också exkluderade från granskningen. Ingen teknisk analys har genomförts och inga stickprov på efterlevnad har tagits.

### 1.4. Metod och genomförande

Granskningens syfte har adresserats genom intervjuer med identifierade nyckelpersoner i de kommunala bolagens IT-säkerhetsarbete samt genomgång av relevant styrdokumentation

(se *Sektion 3. Bilaga: Källförteckning*). Granskningen är utförd mot god praxis inom IT- och informationssäkerhetsområdet samt ett antal revisionskriterier. Revisionskriterierna är de bedömningsgrunder som bildar underlag för granskningens analyser och bedömningar. I denna granskning utgörs revisionskriterierna av:


- ▶ Informationssäkerhetspolicy och relaterade dokument
- ▶ IT-policy och användarinstruktioner
- ▶ IT-strategi
- ▶ Riskanalyser IT
- ▶ Internationella standarder enligt ISO (International Organization for Standardization) avseende ISO 27001:2013 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet
- ▶ Internationella standarder för informationssäkerhet som ryms inom Control Objective for Information and Related Technology Standards (COBIT)


De intervjuade nyckelpersonerna har beretts tillfälle att faktagranska rapporten och lämna synpunkter på dess innehåll. Granskningen har även kvalitetssäkrats av EY:s ansvariga revisor för IT-revision och levererats till Nacka kommuns förtroendevalda revisorer.




## 2. Bedömning avseende svar på revisionsfrågor

Granskningens revisionsfrågor bedöms nedan enskilt för Nacka vatten och avfall AB och Nacka Energi AB i enlighet med matrisens färgkoder. Bedömningen görs med stöd i identifierade observationer och rekommendationer.

 Väsentliga brister har identifierats.

 Brister har identifierats.

 Inga väsentliga brister har identifierats.

### 2.1. Nacka vatten och avfall AB (NVOA)

#### 2.1.1. Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policyers?

Bolaget har inlett arbetet med övergripande styrning och intern kontroll och skapat styrdokument i form av en informationssäkerhetspolicy och en integritetspolicy som både beslutats på relevant nivå av vd:n, och i form av en rutin för säker eposthantering och en IT- och digitaliseringsstrategi som den IT- och digitaliseringsansvarige fastställt. Styrelsen har enligt informationssäkerhetspolicyn ett övergripande ansvar för informationssäkerheten.

I IT- och digitaliseringsstrategin nämns ett systematiskt arbete med informationssäkerhet som en förutsättning för att kunna driva IT- och digitaliseringens fokusområden och för att kunna nå målet om säkra digitala tjänster. Detta stärker säkerhetsarbetets betydelse på organisationens fortsatta förändringresa och höjer kraven på befintliga och nya IT-policyers likväl som medarbetarnas medvetenhet om det. För att öka medvetenheten ytterligare kan befintliga och nya IT-policyers kommuniceras aktivt och regelbundet till alla anställda och vid nyanställning. Vid tillfället saknas en process och rutin som säkerställer detta. IT-policyer är dock tillgängliga på filservern och i intranätet; en genomgång av policyer sker endast på de anställdas egna initiativ och bygger på frivillighet.

Den bolagsspecifika informationssäkerhetspolicyn med utgångspunkt i kommunens motsvarande policy beskriver ansvarsfördelningen gällande styrning, stöd och samordning, och roller inom informationssäkerhetsarbetet. Policyn svarar inte på frågan vilken skyddsnivå mot intrång som anses vara acceptabel och hur den nivån ska säkerställas genom ett systematiskt arbete.

Aktiviteterna som ska genomföras enligt policyn, till exempel systemsäkerhetsanalyser och penetrations tester, är förebyggande och bidrar till en bättre förståelse av NVOA:s risker och hotbild.

NVOA har inlett arbetet med att utveckla och implementera ett ledningssystem för informationssäkerhet (LIS) enligt rekommendation från myndigheten för samhällsskydd och beredskap (MSB). LIS förväntas framöver vara startpunkten för ett mer systematiskt säkerhetsarbete inom NVOA, som förtydligar styrningen och som också ska ge tillfälle att aktualisera informationssäkerhetspolicyn. För nuvarande saknas en rutin för regelbunden översyn av informationssäkerhetspolicyn och av de övriga IT-policyerna. Vid tidpunkten för granskningen ses risken att policyerna utgår från föråldrade legala bestämmelser, branschstandards och annan säkerhetsteknisk kunskap som *låg* eftersom policyerna uppdaterades senast med införandet av dataskyddsförordningen GDPR i maj 2018 eller senare.

Driften av IT sköts av ett upphandlat företag, Basefarm. Frågan om hur NVOA säkerställer att tillräckligt skydd mot intrång finns hos upphandlade företag som sköter driften av IT besvaras i revisionsfråga 8, se sida 16.

## Observationer

Policyer kommuniceras och uppdateras inte aktivt och regelbundet och sätter inte tydliga krav på ansvar, metodik, genomförande, uppföljning och kontroll av informationssäkerhetsaktiviteter.

## Bedömning

Bristerna noteras i sin helhet, dock med hänsyn till att policyer finns på plats på en icke-detaljerad nivå och att verksamheten arbetar med att utveckla informationssäkerheten utifrån dessa.

## Rekommendationer

1. Skapa en rutin för regelbunden översyn av informationssäkerhetspolicyn och övriga informationssäkerhetsrelevanta dokument. Detta inkluderas med fördel i ledningssystemet för informationssäkerhet framöver.
2. Skapa en process och rutin för att kommunicera befintliga och nya IT-policies aktivt och regelbundet till alla anställda och vid nyanställning.
3. Stärk den interna kontrollen genom att sätta periodiska aktiviteter med tydligt ansvar för att verifiera att informationssäkerhetsaktiviteter genomförs ändamålsenligt. Risk- och kontrollmatriser är exempel på verktyg för att sätta tydliga kontroller, ansvar och frekvenser som utgår från bolagets risker och riskaptit. Säkerställ även ansvar för riskhanteringsarbetet.

### 2.1.2. Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?

Informationssäkerhetspolicyn introducerar riskanalyser som en del av bolagets arbete med informationssäkerhet. Målet är att identifiera och bedöma risker vars konsekvenser kan leda till störningar i tillgången till information, allvarliga händelser eller extraordinära händelser. För tillfället genomförs på bolagsnivå dock inte övergripande riskanalyser avseende IT-säkerhet. Huvudanledningen är att det saknas en formaliserad process och ansvar för övergripande riskanalyser på bolagsnivå. Man planerar att åtgärda detta när utvecklingen och implementeringen av LIS gör framsteg.

NVOA har inlett ett internt initiativ att kartlägga bolagets processer där man började dokumentera verksamhetsprocesser och därefter planerar att gå över till stöd- och ledningsprocesser.

NVOA använder sig av runt 40 system varav endast tre ägs av bolaget och anses som verksamhetsspecifika. Hanteringen av övriga system som till exempel HR-systemet ägs av kommunen och används därmed av fler bolag inom Nacka kommun. För de system som ägs av kommunen är NVOA:s möjligheter att påverka riskanalyser begränsade och man har ingen direkt insyn i kommunens arbete med risk- och sårbarhetsanalyser. Det finns ändå ett intresse från bolagets sida och IT- och digitaliseringschefen har nyligen begärt mer information om kommunens arbete med riskanalyser och riskhantering. Frågan om huruvida kommunikationen mellan Nacka kommun och NVOA är ändamålsenlig besvaras också i revisionsfråga 6, se sida 13.

För NVOA:s verksamhetsspecifika system görs riskanalyser avseende IT-säkerhet idag på ett strukturerat sätt. Verksamhetens nuvarande huvudsakliga fokus är att informationsklassa systemen med hjälp av informationsklassningsverktyget KLASSA som Sveriges Kommuner och Landsting (SKL) har tagit fram. KLASSA ger NVOA en plattform att klassificera informationstillgångar utifrån kriterierna tillgänglighet, riktighet, konfidentialitet och

spårbarhet, vilket hjälper verksamheten att förstå hotbilden, skyddsbehov och nödvändiga åtgärdsaktiviteter som sedan fastställs i bolagets handlingsplaner. Verktöget tar hänsyn till lagliga bestämmelser som dataskyddsförordningen GDPR eller direktivet för nätverk och informationssystem (NIS) som är applicerbara för vatten- och avfallsbolag. Risker för intrång ingår explicit i verktygets metodik.

För de verksamhetsspecifika systemen som hittills har bedömts som mest skyddsvärda har NVOA genomfört risk- och sårbarhetsanalyser med hjälp av ett konsultföretag som är specialiserat i IT-säkerhetsfrågor. Risk- och sårbarhetsanalyserna bygger på penetrationstester vilka anses vara ett viktigt verktyg för att kunna förstå bolagets risker och mognadsnivån av befintliga kontroller. Risk- och sårbarhetsanalyserna resulterade i dokumenterade riskbedömningar och rekommendationer. Identifierade gap åtgärdas systematiskt: Till varje system finns en backlog med alla planerade förbättringar och deras prioritering. Systemägarna tar åtgärder enligt prioriteringen.

### Observationer

Verksamheten genomför riskanalyser för "de egna" systemen. För tillfället genomförs på bolagsnivå inte övergripande riskanalyser avseende IT-säkerhet och det finns inte tillräckligt insyn i kommunens arbete med risk- och sårbarhetsanalyser för kommunägda system.

### Bedömning

I sin helhet bedöms dessa brister **inte som väsentliga** med hänsyn till bolagets eget arbete med riskanalyser avseende IT-säkerhet av verksamhetsspecifika system.

## Rekommendationer

1. Fortsätt arbetet med utvecklingen och implementeringen av LIS och införandet av en process för övergripande riskanalyser avseende IT-säkerhet. Säkerställ att ansvarig funktion finns.
2. Fortsätt kartläggningen av bolagets processer, som blir del av grunden för arbetet med verksamhets- och IT-fokuserade riskanalyser och riskhantering.
3. Intensifiera informations- och kunskapsutbyte med kommunen i frågan om risk- och sårbarhetsanalyser för delade system som ägs av kommunen.
4. Fortsätt åtgärda gap som identifierades för verksamhetsspecifika system enligt prioriteringen utifrån de genomförda risk- och sårbarhetsanalyserna.
5. Genomför risk- och sårbarhetsanalyser för verksamhetsspecifika system periodvis för att fånga upp nya risker, kontrollgap och lagliga bestämmelser. Detta kopplas med fördel till den årliga cykeln i ett framtida ledningssystem för informationssäkerhet och/eller operationell riskhantering.

### 2.1.3. Har bolaget ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?

I NVOA:s IT-miljö delas ansvaret för ett ändamålsenligt skydd av databaser och system mellan bolaget, kommunen och IT-driftleverantören Basefarm. Detta medför begränsade möjligheter för NVOA att påverka skyddet mot utomstående intressen eller utifrån kommande hot om skada. Svaret på revisionsfrågan och bedömningen tar hänsyn till detta.

Nätverket som NVOA:s IT ligger i använder sig av segmentering och segregering. Dessa skyddsåtgärder begränsar åtkomsten till känslig information och tjänster för icke-auktoriserade användare.

Segmenteringen sker till exempel i form av separerade administrations- och "IT"-nätverk. De risk- och sårbarhetsanalyser som har genomförts av konsultföretaget med specialisering i informations- och IT-säkerhetsfrågor (se revisionsfråga 2) inkluderar en bedömning av segmenteringens ändamålsenlighet. Analysen upptäckte en brist där ett system låg på administrationsnätverket och inte på IT-nätverket som rekommenderat. Arbetet att åtgärda bristen pågår. Utöver detta finns ett nätverksaktivitets-analysverktyg (Intrusion Detection System, IDS) på plats för att identifiera intrång av obehöriga i nätverket. Som en del av risk- och sårbarhetsanalyserna bedömdes också segregeringens effektivitet. Bolaget gör även egna regelbundna genomgångar av brandväggskonfigureringen.

Den grundläggande behörighetshanteringen sköts via katalogtjänsten Active Directory (AD) som administreras av kommunen, med begränsade påverkningsmöjligheter för NVOA. I AD:t styrs säkerhets- och lösenordsinställningar såsom användarnas administrationsrättigheter inom operativsystemet. I dagsläget ges till exempel alla anställda lokala domänadministrationsrättigheter på sina datorer vilket medger möjlighet att installera, modifiera och avinstallera mjukvaror och förändra vissa inställningar. Därmed ökar risken att anställda installerar skadlig mjukvara som sätter system ur funktion eller underlättar för utomstående användare att komma åt system och information. NVOA är medveten om risken och har inlett diskussioner med kommunen för att åtgärda detta.

Ett kritiskt element av NVOA:s infrastruktur är den tekniska nätinfrastrukturen. Denna har flera åtkomstpunkter vid pumpstationer ute i fält, där åtkomst till vattenledningsinformation och pumpsystem ska vara möjlig för auktoriserade anställda som styr systemen och utför underhåll. Verksamheten har kommunicerat vikten av säkerhetsaspekten till anställda som utför arbetet vilket ökar medvetenheten om relevanta skyddsåtgärder, till exempel att det är viktigt att logga ut efter användande av pumpstationerna.

Ansvar för skydd av databaser och servrar ligger hos IT-driftleverantören Basefarm. Dess interna kontroll bedöms som en del av revisionsfråga 8, se sida 16.

I intervjuerna som fördes på plats nämndes att alla hos Nacka kommun som har en chefsroll inne har tillgång till alla anställdas personuppgifter oavsett om man faktiskt har rollen som närmaste chef eller inte. För att upprätthålla bolagets integritetspolicy och de anställdas integritet bör detta undersökas närmare och nödvändiga åtgärder vidtas om observationen bekräftas.

### Observationer

Det finns/fanns en brist där ett system ligger på fel nätverk. Dessutom ges alla anställda lokala domänadministrationsrättigheter på deras datorer.

### Bedömning

I sin helhet bedöms dessa brister **inte som väsentliga** med hänsyn till pågående åtgärder och bolagets begränsade möjligheter att påverka AD konfigureringen.

## Rekommendationer

1. Upprätthåll segmenteringen av nätverket samt användningen av nätverksaktivitetsanalysverktyget och fortsätt vidta åtgärdande aktiviteter som säkerställer att system ligger i rätt nätverk.
2. Upprätthåll segregeringen av nätverket och fortsätt genomföra periodiska genomgångar av brandväggarnas konfigurering.
3. Ta bort användarnas lokala domänadministrationsrättigheter där dessa inte behövs eller implementera kompenserande kontrollåtgärder som minskar relaterade risker. Fortsätt

dialogen med Nacka kommun.

4. Kommunicera vikten av säkerheten kring kritisk teknisk näsinfrastruktur även framöver och stötta detta genom periodiska utbildningar och tekniska skyddsåtgärder.
5. Undersök chefernas åtkomst till anställdas personuppgifter närmare och inför begränsningar där brister finns.

#### **2.1.4. Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång? Vilka incidenter har inträffat och hur har styrelsen fått kännedom om dessa?**

Enligt informationssäkerhetspolicyn ska alla informationssäkerhetsincidenter anmälas till utpekad funktion och hanteras enligt en definierad incidentprocess. Policyns utformande och syfte ger en tydlig kontext som inkluderar försök till, eller genomförda, intrång i definitionen av informationssäkerhetsincidenter. NVOA har identifierat personuppgiftsincidenter som en särskild incidentkategori med potentiell stora konsekvenser för bolagets rykte och finansiella situation med hänsyn till den nya dataskyddsförordningens bestämmelser och definierade bötesbelopp.

Det finns idag inte någon formell, dokumenterad IT-incidenthanteringsprocess, även om en sådan omnämns i informationssäkerhetspolicyn. För att snabbt kunna eskalera incidenter och inleda riskmitigerande åtgärder bör processen vara dokumenterad, bekant och lättillgänglig för att minska konsekvenser i krissituationer. Incidenter som rör kommunägda system, eller som rör driftleverantörens databaser och servermiljö kommuniceras av Basefarm främst till kommunen. Dessa incidenter hanteras då av kommunen i samarbete med Basefarm. Det saknas en definierad väg och rutin för rapporteringen till NVOA i de fall där anställda hos NVOA använder drabbade system och där incidenten rör NVOA:s verksamhet.

Den särskilda personuppgiftsincidentprocessen är dokumenterad i form av en processkarta med ansvarsfördelning och inblandning av en jurist som bedömer incidentens allvar och konsekvenser. Bolaget har ett verktyg där drabbade kan kontaktas via email och sms och detta kompletteras med en nyhet som publiceras via bolagets/kommunens hemsida och övriga kommunikationskanaler om konsekvensbedömningen kräver detta. Samma verktyg används till verksamhetsincidenter som rör vattenförsörjningen.

Båda incidentprocesser har gemensamt att de inte har kommunicerats fullt ut inom bolaget och att kunskapsnivån kring incidenthantering som konsekvens kan höjas. Ett symptom härav är att anställda tar direkt kontakt med IT- och digitaliseringschefen för att be om råd och information om nödvändiga nästa steg. Här hänvisas de till de definierade processerna.

NVOA har haft några mindre IT- och personuppgiftsincidenter som borttappade datorer. Dessa incidenter bedömdes inte som kritiska och hanterades därför med enkla åtgärder av verksamheten utan att ha rapporterats till styrelsen. I övrigt handlar de flesta incidenter om den faktiska verksamheten. Till dessa finns en etablerad kris- och beredskapsgrupp som sammanställs när behovet finns.

#### **Observationer**

Det finns idag inte någon formell, dokumenterad IT-incidenthanteringsprocess, och incidentprocesser kommuniceras inte tillräckligt. Det saknas en definierad väg och rutin för incidentrapporteringen från driftleverantören och kommunen till NVOA.

#### **Bedömning**

Inom denna fråga noteras brister, med hänsyn till att det finns korta kommunikationsvägar inom bolaget som påskyndar lösningar utan dokumenterade processer och till att det finns en dokumenterad personuppgiftsincidentprocess såsom en kris- och beredskapsgrupp för verksamhetsprocesser.

## Rekommendationer

1. Säkerställa att incidentprocessen för informationssäkerhetsincidenter är dokumenterad, bekant och lättillgänglig, t.ex. som en del av informationssäkerhetspolicyn.
2. Etablera riktlinjer och kommunikationsvägar mellan IT-driftsleverantören, kommunen och bolaget för incidenter som rör NVOA:s verksamhet och system som används av bolaget.
3. Kommunicera incidentprocesser inom verksamheten och säkerställ utbildning av anställda som har en kritisk roll inom hanteringsprocessen.

### 2.1.5. Har tester genomförts avseende intrång i systemen?

Tekniska analyser, så som penetrationstester, definieras som en del av NVOA:s arbete med säker informationshantering i informationssäkerhetspolicyn. Auktoriserade simulerade cyberattacker har genomförts på bolagets datorer som en del av risk- och sårbarhetsanalyser.

Testningens motiv har varit att undersöka möjligheterna att komma åt informationstillgångar. Omfattningen av användarnas lokala domänadministrations-rättigheter har bedömts som riskabel av testaren (se fråga 3, sida 10).

Utöver detta ligger ansvaret hos kommunen för tester för de systemen som ägs av kommunen, och hos IT-driftsleverantören Basefarm för databaser och servermiljö. Revisionsfråga 5 besvaras i revisionsfråga 2 för de system som ägs av kommunen (se delen om risk- och sårbarhetsanalyser, sida 9) och i revisionsfråga 8 för databas och server (sida 16).

### Bedömning

Inga **väsentliga brister** har upptäckts. Stora delar av revisionsfrågan ingår i bedömningen av revisionsfrågorna 3 och 8.

## Rekommendationer

1. Fortsätt genomföra penetrationstester med tillräcklig frekvens enligt egen riskbedömning.

### 2.1.6. Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag samt hur ser kopplingen ut till bolagens interna kontroll?

NVOA har identifierat informationssäkerhet som en prioriterad bolagsaktivitet med egen budget. Informationssäkerhetspolicyn sätter en fördelning av ansvar och roller mellan bolagsstyrelsen, vd:n, enheter, informationsägare, systemägare och systemförvaltare. IT- och digitaliseringsstrategin kompletterar och förtydligar styrningsdokumentet med ytterligare rollbeskrivningar för den IT- och digitaliseringsansvarige, enhetschefer, funktionsansvariga och medarbetare. Ansvar och roller beskrivs mestadels på ett övergripande sätt och kan med fördel i policyarbetet utvecklas för att skapa en starkare individuell medvetenhet om sitt personliga ansvar. För att kunna bedöma organisationen som ändamålsenlig på policynivå



kan den befintliga fördelningen av ansvar och roller förslagsvis kompletteras med kommunikations- och rapporteringsvägar, och med tydliga ansvar på aktivitetsnivå (se revisionsfråga 1, sida 8). Behovet av formella rapporteringsvägar rör främst informationsutbytet med ledningsgruppen och styrelsen. I det dagliga arbetet med informationssäkerhet i verksamheten är arbetet flexibelt med korta och enkla kommunikationsvägar på grund av bolagets storlek.

NVOA befinner sig på en förändringsresa med ett digitaliseringsinitiativ som under det senaste året har lett till en mer dedikerad organisation inom informationssäkerhetsfrågor. En stor milstolpe har nåtts med införandet av ett säkerhetsråd som täcker säkerhetsfrågor i sin helhet för fysisk och digital säkerhet. Detta bedöms vara ett viktigt organisatoriskt framsteg när NVOA ställer om sin infrastruktur och affärsmodell från en analog till en framtidsinriktad digital verksamhet. Informationssäkerhetens roll i organisationen har stärkts ytterligare med en anställd som kartlägger flödet, hantering och lagring av information.

Å andra sidan upplever verksamheten arbetet med informationssäkerhet fortfarande som utmanande på grund av personalbrist. Under vd:n finns ingen riskansvarig som styr arbetet med risk management på den högsta nivån och som knyter säkerhetsriskerna till övriga risker för att skapa ett helhetsperspektiv som hanteras i enlighet med hela bolagets riskaptit. Det har saknats resurser för att systematiskt kunna driva LIS-projektet. Utöver detta ser NVOA behovet att rekrytera ytterligare två IT-nära systemförvaltare som jobbar med verksamhetsspecifika system utifrån ett informationssäkerhetsperspektiv.

En organisation kan endast lyckas med sitt informationssäkerhetsarbete när det förankras i hela verksamheten. Kunskapen behövs byggas ut på alla nivåer genom relevant information och utbildning. Den senaste utbildningen inom informationssäkerhet genomförde NVOA dock för två år sedan. Materialet som användes finns kvar men har inte skickats ut sedan dess och behöver uppdateras. Diskussioner förs om utbildningen ska genomföras mer frekvent och om den ska vara en del av nyanställningsprocessen. Frågan drivs inom LIS-arbetet.

Frågan om NVOA:s organisation är ändamålsenlig behöver dessutom besvaras i en bredare kontext på grund av bolagets organisatoriska och informationstekniska kopplingar till kommunen (se till exempel revisionsfrågor 3 och 4, sida 10): Idag driver bolagets informationssäkerhetsansvarige kommunikationen förhållandevis informellt och informationsutbytet bygger på kontakter från den ansvariges tidigare anställning hos kommunen. Kommunikationen och kunskapen om kommunens arbete med informationssäkerhet är därmed personberoende och det saknas ett organiserat samverkansforum för IT-nära frågor.

Det finns ingen tydlig koppling mellan arbetet med informationssäkerhet och bolagets internkontroll. Internkontrollfunktionen har historiskt inte specifikt tittat på hur NVOA arbetar med informationssäkerhet. 2019 har frågan om informationssäkerhet dock tagits upp av kommunens förtroendevalda revisorer och blivit del av en egen granskning.

### **Observationer**

Policyer specificerar inga kommunikations- och rapporteringsvägar. Verksamheten upplever delvis att det finns en brist på personal som arbetar med informationssäkerhetsfrågor. Det finns inga periodiska utbildningar i dessa frågor. Kunskaps- och informationsutbytet med kommunen är informellt och personberoende.

### **Bedömning**

Ovan noterade brister noteras, med hänsyn till att övergripande policyer finns, att nya resurser och forum finns på plats, att kommunikationen med kommunen sker (även om informellt) och att informationssäkerhet har tagits upp som en fråga i den interna kontrollfunktionen.

## Rekommendationer

1. Utveckla beskrivningar av ansvar och roller i informationssäkerhetspolicyn och komplettera styrdokumentet med kommunikations- och rapporteringsvägar såsom med tydliga ansvar på aktivitetsnivå.
2. Utvärdera behovet av funktioner och resurser inom områdena riskhantering och informationssäkerhet.
3. Öka kommunikationen och informationsutbytet mellan NVOA och kommunen och minska personberoende genom ett strukturerat formellt samarbetsforum i informationssäkerhetsfrågor.
4. Bibehåll informationssäkerhetsfrågan som ett relevant granskningsområde i den interna kontrollfunktionen och genomför granskningar med regelbundenhet utifrån riskbedömningarna.

### 2.1.7. Hur säkerställer styrelsen att den interna kontrollen är tillräcklig och fortlöpande aktuell?

För att säkerställa att den interna kontrollen är tillräcklig och fortlöpande aktuell bör styrelsen sätta tydliga krav på kontrollmiljön och på rapportering, vilken bör innehålla all nödvändig information för att kunna bedöma kontrollmiljöns mognad. Frågan om det finns tydliga krav på kontrollmiljön besvaras i de övriga revisionsfrågorna som noterar att det saknas tydliga krav på metodik och genomförande av informationssäkerhetsaktiviteter, på hur resultat ska följas upp med riskmitigerande åtgärder och på periodiska kontrollaktiviteter för att verifiera att aktiviteterna genomförs ändamålsenligt. Revisionsfråga 7 fokuserar därför på rapporteringen till styrelsen som brukar vara utgångspunkten av en styrelses kontroll över den interna kontrollen. Rapporteringen till styrelsen bör ske frekvent och i tillräckligt utsträckning eftersom informationssäkerhet har identifierats som en prioriterad bolagsaktivitet och eftersom styrelsen har det övergripande ansvaret i frågan.

Den operativa delen av verksamheten som dagligen arbetar med informationssäkerhetsfrågor (första försvarslinjen) har historiskt rapporterat och redogjort sina prioriterade områden och sin progress till styrelsen i form av årliga verksamhetsberättelsen. Berättelsen uppfyller dock inget särskilt kontrollsyfte då det saknas rapporterings- och informationskrav som verksamhetens rapportering bör utgå ifrån. Rapporteringen bör utgå från sådana krav och ske frekvent för att redovisa att kontrollen är tillräcklig. I ett första skede krävs att tydliga kontrollaktiviteter fastställs, se tidigare observationer och rekommendationer i denna rapport.

En funktion för risk management och compliance (andra försvarslinjen) är inte på plats (se revisionsfråga 6, sida 13). Ansvaret lämnas därmed till vd:n, och dess rapportering utgår inte från tydliga krav som avser rapportering i frågan om informationssäkerhet.

Bolagets internkontrollfunktion (tredje försvarslinje) har historiskt inte specifikt tittat på hur NVOA arbetar med informationssäkerhet och inte rapporterat i frågan.

#### Observationer

Det saknas tydliga krav på kontrollmiljön, kontrollaktiviteter och rapporteringen från styrelsens sida.

#### Bedömning

I sin helhet bedöms dessa brister som **väsentliga**.



## Rekommendationer

1. I styrelsen, sätt tydliga krav på kontrollmiljön och kontrollaktiviteter.
2. I styrelsen, sätt tydliga krav på rapporteringen från relevanta aktörer, särskilt gällande styrelsens informationsbehov och efterfrågad rapporteringsfrekvens.
3. Säkerställ att ansvarig funktion för risk management och compliance (riskhantering och regeluppfyllnad) finns.

### 2.1.8. Hur säkerställs att tillräcklig intern kontroll finns hos upphandlade företag som sköter driften av IT?

NVOA:s IT- och digitaliseringsansvarige har rollen som kravställare av säkerhet på nya digitala tjänster och system. Denne ska konsulteras vid inköp och leder även kontakter och arbete mellan verksamheten och IT-leverantörer. Ansvar fastställs idag i IT- och digitaliseringsstrategin och bör även explicit utökas till befintliga upphandlade digitala tjänster och system för att säkerställa att det finns utpekat ansvar för informationssäkerheten för alla tjänster och system efter inköpet, och att ansvaret är tydligt.

Idag använder NVOA Basefarm som det enda upphandlade företaget som sköter driften av IT. Huvudavtalet upphandlades av Nacka kommun för samtliga verksamheter och enheter inom kommunen. Detta omfattar ett helhetsåtagande för IT-drift vilket innebär ansvaret för ägarskap och underhåll av bakomliggande infrastruktur och teknik. I helhetsansvaret ingår skydd för databaser och system mot utomstående intressen samt för intrång eller utifrån kommande hot om skada. Detta ska enligt avtalet utformas utifrån lagliga krav och gällande branschstandards.

Huvudansvaret för att säkerställa att tillräcklig intern kontroll finns hos Basefarm ligger hos Nacka kommun som är kontraktspartner och ägaren av majoriteten av systemen som används i NVOA:s verksamhet. NVOA förlitar sig delvis på att kommunen uppfyller sin kontrollfunktion, vilket anses vara lämpligt, och gör utöver detta även ansträngningar för att följa upp kommunens arbete som kontrollägare, till exempel när det gäller kommunens risk- och sårbarhetsanalyser för kommunägda system (se revisionsfråga 2, sida 9).

NVOA ska kontrollera Basefarm för de system som är verksamhetsspecifika, t.ex. bolagets skadesystem. Bolaget har ställt vissa krav på aktivitetsloggning och tänker framöver även verifiera att åtkomsten till serverhallen är begränsad till auktoriserade och lämpliga individer. Inom organisationen saknas dock detaljerad kunskap om driftavtalets innehåll och därmed om omfattningen av NVOA:s kontrollansvar som uppstår när driften outsourcas. Basefarm bör t.ex. på eget initiativ genomföra penetrationstester, men NVOA saknar insyn om tester har genomförts för verksamhetsspecifika system och infrastrukturen.

#### Observationer

Den IT- och digitaliseringsansvariges ansvar som kravställare av informationssäkerhet appliceras formellt inte till befintliga upphandlade digitala tjänster och system. Inom NVOA saknas detaljerad kunskap om driftavtalets innehåll och därmed om omfattningen av bolagets kontrollansvar.

#### Bedömning

I sin helhet bedöms detta som brister, med hänsyn till att en stor del av kontrollansvaret ligger hos kommunen och med hänsyn till att vissa krav på kontrollnivån ställs från bolagets sida.

## Rekommendationer

1. Utöka den IT- och digitaliseringsansvariges ansvar som kravställare på säkerhet formellt till redan upphandlade tjänster och system.
2. Fortsätt kontrollera att Basefarms internkontroll är tillräcklig där det finns ett kontrollansvar hos NVOA och där påverkningsmöjligheter finns.
3. Systematisera NVOA:s kontrollarbete av upphandlade leverantörer med dokumenterade krav och aktiviteter som har sin utgångspunkt i kontrakten.

## 2.2. Nacka Energi AB (NEAB)

Sammanfattningsvis kan sägas att Nacka Energi AB har mycket på plats, men att de tekniska åtgärderna och kontrollerna bör kompletteras med formell dokumentation och formella processer för styrning.

### 2.2.1. Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policyer?

Bolaget har inlett arbetet med övergripande styrning och intern kontroll i och med att ledningsgruppen har beslutat en informationssäkerhetspolicy som är NEAB:s centrala styrdokument och som arbetet med skydd mot intrång ska utgå ifrån.

Enligt policyn har koncernchefen och vd:n det övergripande ansvaret för koncernens och bolagets nivå av informationssäkerhet.

Enligt informationssäkerhetspolicyn anser ledningen att tydliga rutiner för informationshantering och medarbetares agerande är en förutsättning för att kunna begränsa säkerhetsrisker. Bolaget har bland annat implementerat dokumenterade rutiner för behörighetstilldelning till IT-system och en upphandlingspolicy. Det finns även en policy för digital kommunikation och sociala medier. För att öka medvetenheten om policyernas innehåll delges de till nyanställda och t.ex. vid gemensamma möten och vid konferenser. De finns också tillgängliga på en intern filserver.

För nuvarande saknas en rutin för periodisk översyn av informationssäkerhetspolicyn och av de övriga IT-policyerna. En ansvarig för hantering av styrdokument o.dyl. är dock nyligen tillsatt. Vid tidpunkten för granskningen är risken att policyerna utgår från föråldrade lagliga bestämmelser, branschstandards och annan säkerhetsteknisk kunskap låg då de uppdaterades senast i och med införandet av dataskyddsförordningen GDPR i maj 2018.

De befintliga dokumenten är beslutade av ledningsgruppen men utgår inte från kommunkoncernens IT-policyer - med undantag av rutinen för behörighetstilldelning och upphandlingspolicyn. En anledning till detta är att kommunen och kommunkoncernens policyarbete har varit under utveckling. I de fallen där NEAB:s styrdokument har en tydlig koppling till kommunens eller koncernens policyer har bolaget själv efterfrågat mallar, vilket bedöms vara ett viktigt samarbetsorienterat initiativ som hjälper till att standardisera och effektivisera processer inom Nacka kommun, dess koncern och dess bolag.

Informationssäkerhetspolicyn fastställer ambitionen att implementera tydliga rutiner senast i juni 2019. NEAB uppfyller inte ambitionen än. Det pågår ett arbete med att säkerställa och upprätta policyer där det saknas, enligt ISO27000 och KLASSA. Rutiner för riskanalyser genomförs i enlighet med EI:s, SVK:s och MSB:s instruktioner, det skulle även vara önskvärt att detta förtydligas i informationssäkerhetspolicyn.

Den delen av organisationen som arbetar med informationssäkerhetsfrågor är medveten om befintliga brister på dokumenterade rutiner och har skapat en lista över dessa. Listan visar organisationens fortsatta fokus på förbättringspotential och bör aktualiseras framöver; informationssäkerhet prioriteras internt.

Sedan november 2018 arbetar NEAB med att implementera direktivet för nätverk och informationssystem (NIS) med beröringspunkter till säkerhetsstandarden ISO 27001 och målet att få till omfattande styrdokument och rutiner. Detta projekt strävar inte efter en ISO certifiering men utgår ifrån att organisationen når en bra skyddsnivå om standardens krav uppfylls. Just nu identifierar och kartlägger NEAB vilka delar av standarden som redan finns på plats. Enligt den senaste tidsplaneringen ska bolaget innan årsslutet ha skaffat sig en bättre förståelse över hur väl bolaget uppfyller kraven i ISO 27001. Ett resultat av arbetet ska vara en lista med prioriterade förbättringsområden som arbetet med informationssäkerhet bör fokusera på framöver. Större initiativ ska få en egen budget. Att implementera fler

styrande och ändamålsenliga dokument är ett av de identifierade fokusområden.

### **Observationer**

Det finns tydliga och ändamålsenliga styrdokument. Dock är inte alla styrdokument på plats än. Policyer uppdateras inte aktivt och regelbundet, dock uppdateras de då händelser föranleder detta.

### **Bedömning**

Ovan noteras som brister; med hänsyn till att policyer finns på plats, att verksamheten arbetar med informationssäkerhet utifrån dessa, att det finns dokumenterade kravlistor på IT-säkerhet, och att det finns en pågående förändringsresa där man kartlägger bristerna.

## **Rekommendationer**

1. Skapa en rutin för regelbunden översyn av informationssäkerhetspolicyn och övriga relaterade styrdokument. Detta inkluderas med fördel i ett ledningssystem för informationssäkerhet framöver.
2. Stärk den interna kontrollen genom att sätta periodiska aktiviteter med tydligt ansvar för att verifiera att informationssäkerhetsaktiviteter genomförs ändamålsenligt.

### **2.2.2. Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?**

Enligt informationssäkerhetspolicyn ska den risknivån som verksamheten utsätts för vara medvetet vald, vilket sätter ett tydligt krav på att riskanalyser ska genomföras på ett strukturerat sätt och omfatta risker för intrång. Riskanalyser genomförs i enlighet med EI:s och SVK:s krav, dock är den dokumenterade processen (med aktiviteter och roller/ansvar) på gång. Roller och ansvar kommer att sättas på plats i och med arbetet med ISO27000-implementering.

Riskbedömningar i det operativa arbetet bör utgå ifrån bolagets mål och riskaptit och ta ett helhetsperspektiv för att kunna balansera bolagets risker: Acceptans för en högre risk i ett projekt kan t.ex. kompenseras genom ytterliga skyddsåtgärder i övrigt.

I intervjuerna anges att risker analyseras informellt enligt vedertagen praxis och att man har hanterat och fortfarande hanterar risker, till exempel i samband med införandet av nya system eller uppgraderingar.

Bristerna ingår idag som ett av NEAB:s framtida fokusområden i NIS-projektet. Det är tänkt att införa en egen utbildning kring hur riskanalyserarbetet ska hanteras.

I samband med införandet av dataskyddsförordningen har NEAB kartlagt personlig information i sina system i form av en registerförteckning. Bolaget har dock inte genomfört bredare informationsklassningar av sina system för att kunna identifiera och bedöma känslig information som inte är personlig

### **Observationer**

För tillfället genomförs riskanalyser avseende IT-säkerhet i enlighet med EI:s och SVK:s

krav. Dock är dokumentationen kring detta under arbete.

### **Bedömning**

Detta noteras som brist. Dock kommer den nya rollen, och resultatet av NIS-projektet (som hanterar införande av ISO27000 och KLASSA) att åtgärda detta.

## **Rekommendationer**

1. Utveckla, dokumentera och implementera en formell process för övergripande riskanalyser avseende IT-säkerhet.
2. Genomför informationsklassningar enligt definierade kriterier.

### **2.2.3. Har bolaget ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?**

NEAB använder sig av en kombination av olika åtgärder för att stärka skyddet av sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada. Fysisk säkerhet, nätverkssegmentering, nätverkssegregering, en ändamålsenlig behörighetsstruktur och en definierad behörighetstilldelningsprocess med separerade ansvarsområden, funktioner och arbetsuppgifter ingår som viktiga delar i kombinationen.

NEAB hanterar driften internt med egen personal och konsulter. Detta upplägg medför att den fysiska säkerheten ingår i bolagets kontrollansvar för att förhindra icke-auktorerad tillgång till databaser och system. Serverrum och datahall är utrustad för säkerhet genom ett larmsystem och en dubbel autentisering som kräver att en anställd verifierar sig både med ett fysisk kort och en digital kod innan dörren öppnas. För att minska risken att tillgångsbehörigheter ligger kvar trots organisatoriska förändringar har säkerhetssystemet en funktion för tidsstyrda koder och den används t.ex. till konsulter. NEAB utvecklar den fysiska säkerheten fortsatt och har precis tagit beslut av att klassa personal: Konsulter anses inte längre som personal och deras åtkomst avgränsas till enbart projekt som de arbetar inom. Klassningen tittar också på vilka anställda som kommer att behöva gå igenom registerkontroller. Detta arbetet är påbörjat.

Nätverket som NEAB:s IT ligger i använder sig av segmentering och segregering. Dessa skyddsåtgärder begränsar åtkomsten till känslig information och tjänster genom att hindra icke-auktorerade användare från att röra sig fritt i nätverket. Segmenteringen sker till exempel i form av separerade kontors-, mät-, gäst-, server- och backupnätverk och i form av en demilitariserad zon (DMZ). Det finns ett nätverksaktivitetsanalysverktyg (Intrusion Detection System, IDS) på plats för att identifiera intrång av obehöriga i nätverken.

Bolaget gör regelbundna genomgångar av konfigurationen för samtliga brandväggar för att bedöma nätverkssegregeringens effektivitet. En extern part utför dessa genomgångar med fördel av att ha en mer oberoende granskning med nödvändig kompetens. Samma regelbundna rutin används till genomgångar av routrar. Processen är planerad att vara klar och implementerad till 1a oktober.

Databaser och system utsätts inte endast för hot i form av externa användare som skaffar sig åtkomst till infrastrukturen, utan också i form av interna användare som har tillgång till information som antingen är känslig eller som inte behövs av användare för att kunna utföra sina dagliga arbetsuppgifter. Detta ska styras genom en ändamålsenlig behörighetsstruktur vilket har varit och är ett viktigt fokusområde av NEAB:s arbete i GDPR- och NIS-projekten. För att skydda känslig information har man i samband med dataskyddförordningens införande tagit fram en registerförteckning för alla system och som en teknisk och organisatorisk säkerhetsåtgärd tittat på hur man med behörigheter kan begränsa åtkomst till den kartlagda informationen i systemen. Med hänvisning till att informationsklassningar inte

har genomförts för icke-personlig information bör detta viktiga arbetet utökas till all annan känslig information i systemen (se revisionsfråga 2, sida 19).

Behörigheterna tilldelas och styrs enligt en dokumenterad rutin för behörighetstilldelning till IT-system. Enligt rutinen administrerar IT-organisationen behörigheter. IT-organisationen initierar behörighetsförändringar endast med anledning av att det finns en dokumenterad behörighetsbeställning som är godkänt av den anställdas linjeförman, eller med anledning av att organisatoriska förändringar (t.ex. avgångar) kommuniceras till IT-organisationen. Dessa kontroller är väsentliga och vanliga IT-generella kontroller som minskar intrångsrisken. Övriga väsentliga IT-generella kontroller saknas i den dokumenterade rutinen. Ett exempel är periodiska genomgångar som minskar risken att behörigheter ligger kvar efter organisatoriska ändringar (t.ex. avslutningar) eller genomgångar av lösenordsinställningar.

### Observationer

Tidigare genomgångar av brandväggskonfigureringar har inte alltid dokumenterats. Det saknas informationsklassningar som kan vara utgångspunkt till att man skyddar känslig information genom modifierade behörigheter. Några rekommenderade IT-generella kontroller ingår inte i rutinen för behörighetstilldelning.

### Bedömning

Inga väsentliga brister noterade; med hänsyn till att skyddet mot intrång bygger på en kombination av fysisk säkerhet, nätverkssegmentering, nätverkssegregering, ändamålsenliga behörighetsstrukturer och behörighetsprocesser som i stort sätt bör säkerställa skydd för databaser och system.

## Rekommendationer

1. Upprätthåll segmenteringen av nätverket samt användningen av nätverksaktivitetsanalysverktyget.
2. Upprätthåll segregeringen av nätverket och fortsätt genomföra periodiska genomgångar av brandväggarnas konfigurering. Dokumentera genomgångar på ett strukturerat och standardiserat sätt.
3. Inkludera övriga vanliga och viktiga IT-generella kontroller i rutinen för behörighetstilldelning och uppfylls dess krav. Det rekommenderas att periodiska genomgångar av alla behörigheter ingår i behörighetsrutinen och att de genomförs årligen för vanliga behörigheter och två gånger om året för privilegierade behörigheter. Utöver detta rekommenderas periodiska genomgångar av lösenordsinställningar.

### 2.2.4. Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång? Vilka incidenter har inträffat och hur har styrelsen fått kännedom om dessa?

Enligt informationssäkerhetspolicyn ska det finnas en rutin för säkerhetsincidenter. I policyn ses säker IT- infrastruktur och IT-drift som en förutsättning till bra informationssäkerhet, därmed ingår försök till eller genomförda intrång i definitionen av säkerhetsincidenter.

Det finns idag inte någon formell, dokumenterad incidenthanteringsprocess, även om en sådan omnämns i informationssäkerhetspolicyn. De som arbetar med informationssäkerhet hos NEAB har tidigare ansett detta som tillräckligt på grund av att man har varit ett litet bolag utan större behov av formell struktur inom incidenthantering. För att snabbt kunna eskalera incidenter och inleda riskmitigerande åtgärder bör processen dock vara dokumenterad, bekant och lättillgänglig för att minska konsekvenser i krissituationer. NEAB:s tankesätt har redan nu delvis förbättrats som en konsekvens av att informationssäkerhet har blivit en



prioriterad aktivitet i bolaget och blivit mer strukturerat i det påbörjade arbetet med NIS-direktivet där man planerar att dokumenterade incidentrutiner ska vara på plats framöver. Kunskap om incidenthantering finns redan idag i den delen av organisationen som arbetar med informationssäkerhet: IT-chefen, IT- och säkerhetsmanagern och två IT-driftstekniker har deltagit i en utbildning om processer för incidenthantering, också utifrån NIS-direktivets krav. Denna kunskap bör utnyttjas i arbetet med dokumenterade rutiner framöver.

Hittills har NEAB internt använt sig av informella arbetssätt för att hantera de incidenter som har inträffat. Bolaget har t.ex. blivit mål för DDOS attacker som har påverkat åtkomsten till systemen och information. Driftstekniker hanterade incidenterna utifrån sin egen kunskap och erfarenhet. Samma arbetssätt används fortsatt till incidenter idag. Utöver det har NEAB tillgång och budget för att kunna ta hjälp från externa leverantörer, rådgivare och andra experter i de fall där relevant kunskap eller teknik saknas.

Säkerhetsincidenterna visade också att det finns en kultur inom organisationen där man eskalerar incidenter: Incidenter rapporteras enligt kraven i NIS, GDPR (här finns formell dokumenterad process) och säkerhetsskyddslagen till berörda myndigheter. Internt eskaleras de informellt eller formellt till IT-chefen som rapporterar vidare till VD eller ledningen - som har rapporteringsansvaret mot styrelsen. IT-organisationen anser det viktigt att vd:n får kännedom om incidenter.

De informella arbetssätt som finns bör dock ändå finnas dokumenterade för att kunna minska personberoendet och för att lättare kunna säkerställa effektiva och standardiserade hanterings- och rapporteringsprocesser. Rutinerade och dokumenterade processer är även viktiga för att säkerställa att de befintliga mallar som är utformade, t.ex. utifrån lagliga krav vid personuppgiftsincidenter, används.

### **Observationer**

Det finns idag inte någon formell, dokumenterad säkerhetsincidenthanteringsprocess. Rapportering av incidenter ligger inbakat i linjeorganisationens struktur.

### **Bedömning**

Ovan observation noteras som brist; med hänsyn till att det finns korta kommunikationsvägar inom bolaget som påskyndar lösningar utan dokumenterade processer och till att det finns en kultur som värdesätter rapportering och samarbete i incidentfall. Utöver detta har resan till mer standardiserade processer påbörjats i form av en gemensam utbildning och inom NIS-projektet. Givet NEAB:s storlek ses nuvarande struktur vara funktionell.

### **Rekommendationer**

1. Säkerställ att incidentprocessen för informationssäkerhetsincidenter är dokumenterad, bekant och lättillgänglig, t.ex. som en del av informationssäkerhetspolicyen.
2. Fortsätt eskalera incidenter inom verksamheten och säkerställa utbildning av anställda som har en kritisk roll inom hanteringsprocessen. Kommunikations- och rapporteringsvägar kan formaliseras som en del av incidentprocessen.

#### **2.2.5. Har tester genomförts avseende intrång i systemen?**

Risk- och sårbarhetsanalyser definieras som en förutsättning till bra informationsarbete i NEAB:s informationssäkerhetspolicy. Tekniska tester som t.ex. penetrationstester som

bedömer bolagets sårbarhet avseende intrång i systemen bör ingå i sådana analyser. Tester avseende intrång har dock sist genomförts för ca 15 år sedan. Organisationen förlitar sig i dag huvudsakligen på automatiska notifieringar från befintliga brandväggsloggar och på det installerade nätverksanalysverktyget (IDS, se revisionsfråga 3, sida 20).

IT- och säkerhetsmanagern har dock vid slumpmässiga tillfällen genomfört portskanningar hemifrån för att utvärdera möjligheter att komma åt information utan auktorisering.

### **Observationer**

För tillfället genomförs inga systematiska, dokumenterade penetrationstester eller likande tester avseende intrång i systemen. Vid förändringar i systemmiljön genomförs dock tester enligt praxis.

### **Bedömning**

Bristen noterad. Se rekommendation.

## **Rekommendationer**

1. Analysera behovet av att genomföra systematiska, dokumenterade penetrationstester med tillräcklig frekvens enligt egen riskbedömning.

### **2.2.6. Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag samt hur ser kopplingen ut till bolagens interna kontroll?**

NEAB har identifierat informationssäkerhet som en prioriterad bolagsaktivitet med egen budget. Informationssäkerhetspolicyn sätter en fördelning av ansvar och roller, främst mellan koncernchefen, vd:n, informationssäkerhetssamordnare, (IT-)säkerhetschefen, driftchefen, informationsägare, systemägare och systemförvaltare. Ansvar och roller beskrivs dock mestadels på ett övergripande sätt. Styrelsens ansvar fastställs inte i policyn.

I det dagliga arbetet fylls rollerna främst av en IT-chef som ansvarar för arbetet med informationssäkerhet. Denna person stöds av en IT-drifttekniker med specialkompetens gällande säkerhet. Det finns dessutom drifttekniker som t.ex. uppdaterar datorer, mobiler och servrar, och som sköter driften av routrar och infrastrukturen.

GDPR-ansvarig ingår i ekonomiavdelningen. De som arbetar med informationssäkerhet hos NEAB upplever att ledningen är positiv till arbetet och tilldelar budget efter behov för att kunna ta in den kompetens som behövs. En säkerhetskonsult och en konsult med erfarenhet från NEAB:s IT-miljö är t.ex. involverade i NIS projektet.

De som samordnar och leder informationssäkerhetsarbetet är medvetna om att bolagets framgång i säkerhetsfrågor och på digitaliseringsresan beror på hur man lyckas med att involvera hela organisationen i arbetet med informationssäkerhet. För att öka medvetenheten bland NEAB:s anställda förklarar den informationssäkerhetsansvarige till bolagets anställda de förändringar som ökar säkerheten. Detta gjordes t.ex. när man reducerade tiden efter vilken en anställds dator automatiskt låses i dess frånvaro. Mer strukturerad utbildning av alla anställda finns i form av en digital utbildning inom GDPR som sker regelbundet och som innehåller en egen del om säkerhet. Detta uppfyller informationssäkerhetspolicyns krav på en egen GDPR utbildning.

För att uppfylla policyns krav på att medarbetare ska ges kännedom om betydelsen av informationssäkerhet kan utbildningen i informationssäkerhet dock behöva utökas. I dagsläget finns det planer att införa MSB:s datorstödda informationssäkerhets-utbildning för användare (DISA) med bl.a. ytterligare information om nätverk och informationssystem.



I övrigt är NEAB:s organisation samarbetsorienterad och Kooperationer används till bolagets fördel. Det finns ett bra samarbete med (mjukvara-)leverantörer där man använder leverantörernas kompetens som stöd för att höja informationssäkerhet inom ramen för leverantörernas tjänster och produkter. Ett annat exempel från lyckade samarbeten är Kooperationen med Säkerhetspolisen som har varit närvarande på företagets informationssäkerhetskonferenser med alla anställda.

Bolagets internkontrollfunktion (tredje försvarslinje) har de senaste 15 åren inte specifikt tittat på hur NEAB arbetar med informationssäkerhet och inte rapporterat i frågan. 2019 har frågan om informationssäkerhet dock tagits upp av kommunens förtroendevalda revisorer och blivit del av en egen granskning. De som leder och arbetar med informationssäkerhet är positivt inställda till en återkommande internrevision som anses vara ett värdefullt verktyg för att öka medvetenheten om frågan i styrelsen, ledningen och den övriga organisationen.

### **Observationer**

Policyer beskriver ansvar och roller på ett övergripande sätt. De kompletteras med befattningsbeskrivningarna. Det saknas information om styrelsens ansvar. Rapporteringssvårigheter är satta utefter organisationsstrukturen.

### **Bedömning**

Inga väsentliga brister noterade.

## **Rekommendationer**

1. Utveckla informationssäkerhetspolicyn med tydligare information om styrelsens ansvar.

### **2.2.7. Hur säkerställer styrelsen att den interna kontrollen är tillräcklig och fortlöpande aktuell?**

Vid rapportering till EI och SVK angående RSA:er informeras styrelsen av rapporten i enlighet med kraven i styrelsens arbetsordning.

Styrelsen har historiskt sett även vid specifika händelser och upphandlingar krävt förklaringar från den operativa delen av verksamheten som dagligen arbetar med informationssäkerhetsfrågor (första försvarslinjen) och IT-chefen har ansvarat för att dessa förfrågningar besvaras. Ett exempel har varit vid inköp av nya system där styrelsen krävde insyn i riskanalyser och de åtgärder man tog för att säkerställa att upphandlingen skedde ändamålsenligt. I och med att incidenter rapporteras till styrelsen (se revisionsfråga 4) bad styrelsen i ett fall om insyn i NEAB:s integrationer och IT-organisationen redogjorde hur och varför incidenter har uppstått genom att man skapade schematiska bilder.

Rapporteringen bör utgå från sådana krav och ske mer frekvent för att redovisa att kontrollen är tillräcklig. I ett första skede krävs att tydliga kontrollaktiviteter fastställs, se tidigare observationer och rekommendationer i denna rapport.

Bolagets internkontrollfunktion (tredje försvarslinje) har historiskt inte specifikt tittat på hur NEAB arbetar med informationssäkerhet och inte rapporterat i frågan.

### Observationer

Det finns krav på regelbunden rapportering inom olika områden, samt vid specifika typer av händelser.

### Bedömning

Inga väsentliga brister noterade.

## Rekommendationer

1. I styrelsen, sätt tydliga krav på rapporteringen från relevanta aktörer, särskilt gällande styrelsens informationsbehov och efterfrågad rapporteringsfrekvens.

### 2.2.8. Hur säkerställs att tillräcklig intern kontroll finns hos upphandlade företag som sköter driften av IT?

Driften av NEAB:s nuvarande IT-miljö sköts internt vid behov med stöd av konsulter. I övrigt finns det etablerade supportavtal för de flesta leverantörer som stöttar i driften av IT. Kommunens upphandlingsenhet anlitas vid behov vid upphandling av nya system.

Det finns en beslutad upphandlingspolicy som uppmanar beställare och upphandlare att dokumentera funktionella och tekniska aspekter i upphandlingar av IT-utrustning och IT-system. Informationssäkerhet listas som en aspekt att ta hänsyn till och flera punkter ingår i informationssäkerhetsaspekten. Majoriteten av aspekterna och deras punkter i policyn är dock inga tydliga krav utan formulerat som öppna frågor som beställaren bör fundera över. Exempelvis ställs frågan om hur säkerhetskopieringen ska hanteras, eller t.ex. om aktiviteter ska loggas. Detta istället för att policyn själv kräver frekventa säkerhetskopior och loggning av privilegierade användare enligt en dokumenterad IT-policy. Dessutom rekommenderar policyn beställaren och upphandlaren endast att ta kontakt med IT-avdelningen för att säkerställa rätt kunskap och stöd i upphandlingen. IT-avdelningen har därmed per policy en rådgivande och kravställande roll avseende informationssäkerhet. NEAB:s säkerhetskrav vid upphandling finns dokumenterad i en checklista, vilken dock inte är en officiell bilaga till upphandlingspolicyn och inget obligatoriskt dokument till upphandlingar. Detta för att det skiljer så mycket mellan olika upphandlingar så att det inte är praktiskt görbart att ha en generisk lista för alla.

Supportavtalen som finns reglerar krav på hantering av känslig eller personlig information (t.ex. kryptering) såsom krav på uppkoppling och inloggning – t.ex. sätter NEAB krav på att alla leverantörer ska använda personliga inloggningar och inga systemkonton. Avtalen kräver även att leverantörer ska följa NEAB:s informationssäkerhetspolicy och säkerhetsregler och att leverantörerna bär kostnaderna i de fall där leverantören inte uppfyller GDPR:s kraven. Kontroll av leverantören och en fortsatt dialog med leverantörerna säkerställs för vissa system genom periodiska förvaltningsmöten och genom ett antal icke formaliserade möten. Frekvensen beror t.ex. på hur mycket utveckling som sker till ett system (t.ex. har man velat ha mer frekventa möten för att säkerställa god support och säkerhet till kundsystemet). Varken i informationssäkerhetspolicyn eller i upphandlingspolicyn ställs dock krav på att periodiska uppföljningar ska göras för att säkerställa att leverantörer efterlever säkerhetskraven.

I tidigare fall där NEAB har identifierat att vissa leverantörer inte uppfyller kraven har detta diskuterats med leverantören och krav på åtgärder har ställts. I vissa fall har NEAB även slutat samarbetet med leverantörer som inte har uppfyllt kraven.

### **Observationer**

NEAB sköter driften av IT själva, supportavtalen reglerar hantering där det skulle kunna bli relevant.

### **Bedömning**

I och med att driften sköts internt blir denna fråga delvis irrelevant.

### **Rekommendationer**

1. Säkerställ att NEAB via avtal täcker relevanta krav gentemot leverantörer då det eventuellt är/blir relevant.

### 3. Bilaga: Källförteckning

#### 1. Intervjuade roller

##### 1.1 Nacka vatten och avfall AB (NVOA)

- ▶ IT- och Digitaliseringschef
- ▶ Ekonomichef

##### 1.2 Nacka Energi AB (NEAB)

- ▶ IT-chef
- ▶ IT- och Säkerhetsmanager

#### 2. Dokumentation

##### 2.1 Nacka vatten och avfall AB (NVOA)

- ▶ Begäran om registerutdrag (mall)
- ▶ Huvudavtal mellan Nacka Kommun och Basefarm AB avseende leverans av IT-drift inkl. kapacitetstjänster, driftstjänster, samverkan support, konsulttjänster, SLA, transition samt bilaga 3 (Service, support, SLA) och personuppgiftsbiträdesavtal
- ▶ Rutin för säker eposthantering
- ▶ Informationssäkerhetspolicy
- ▶ Integritetspolicy
- ▶ IT- och Digitaliseringsstrategi Nacka vatten och avfall AB
- ▶ Process för personuppgiftsincident
- ▶ Process för registerutdragsbegäran
- ▶ Registerutdrag från Nacka vatten och avfall (mall)

##### 2.2 Nacka Energi AB (NEAB)

- ▶ Policy för informationssäkerhet
- ▶ Upphandlingspolicy inkl. Appendix (beskrivning av NEAB:s tekniska miljö)
- ▶ Digital kommunikation – Instruktion för användare
- ▶ Policy för sociala medier
- ▶ Rutiner för behörighetstilldelning, IT-system
- ▶ Ansvarsförbindelse för användning av Nacka Energi AB:s digitala resurser och medgivande att hantera personadresserad post (mall)
- ▶ Beställningslista IT för nyanställd
- ▶ Informations- och IT-säkerhetskrav – Basnivå
- ▶ Informations- och IT-säkerhetskrav – Utökad nivå
- ▶ Säkerhetskrav Upphandling – Basnivå
- ▶ Loggning brandvägg
- ▶ Behandling av uppgifter om anställda vid Nacka Energi AB – information enligt dataskyddslagstiftningen
- ▶ Säkerhet i Nacka Energis lokaler
- ▶ Ej dokumenterade rutiner
- ▶ Dokumentation täckandes förvaltningsorganisation och processer kopplade till GDPR
- ▶ Myndigheten för samhällsskydd och beredskap – MSB:s skrift "Vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen"
- ▶ Energimarknadsinspektionens – EI:s skrift "Handbok för redovisning av risk- och sårbarhetsanalys samt åtgärdsplan"
- ▶ Svenska Kraftnät – Svk:s skrift "Vägledning för risk och sårbarheter i elsektorn"

Lekmannarevisorerna

2019-09-11









Till: Styrelse och VD i Nacka vatten och avfall

För kännedom: Kommunstyrelsen och kommunfullmäktige


**Granskning av IT-säkerhet**


EY har på uppdrag av lekmannarevisorerna i Nacka vatten och avfall AB genomfört en granskning av hur bolaget arbetar med IT-säkerhet. Granskningens syfte har varit att ge en övergripande nulägesbild av huruvida Nacka kommuns Kommunstyrelse och bolagets ledning har tillsett att arbetet med IT-säkerhet bedrivs ändamålsenligt och om det finns tillräcklig styrning och intern kontroll avseende skydd mot intrång i bolagets IT-system.

Granskningen har utgått från SIO270001-standarderna och har omfattat 8 revisionsområden. Sammanfattningsvis är resultatet av granskningarna enligt följande:

Revisionsfråga	NVOA
1. Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policies?	
2. Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?	
3. Har bolagen ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?	
4. Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång? Vilka incidenter har inträffat och hur har styrelsen fått kännedom om dessa?	
5. Har tester genomförts avseende intrång i systemen?	
6. Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag samt hur ser kopplingen ut till bolagens interna kontroll?	
7. Hur säkerställer styrelsen att den interna kontrollen är tillräcklig och fortlöpande aktuell?	
8. Hur säkerställs att tillräcklig intern kontroll finns hos upphandlade företag som sköter driften av IT?	

**Färgkoder**
 Väsentliga brister har identifierats.

 Brister har identifierats.

 Inga väsentliga brister har identifierats.

Utifrån granskningsresultatet rekommenderar vi bolaget att vidta åtgärder för att stärka den interna kontrollen. Det är särskilt viktigt att styrelsen aktivt säkerställer en tillräcklig intern kontroll inom området.

Vi önskar kommentarer samt åtgärdsplan med tidplan från bolaget senast den 15 november 2019.

För lekmannarevisorerna

  
Yvonne Wessman  
Ordförande

  
Lars Berglund  
Vice ordförande

Bilaga: Rapport- granskning av IT-säkerhet i de kommunalägda bolagen Nacka vatten och avfall AB och Nacka Energi AB