Revisionsrapport 2022
Genomförd på uppdrag av revisorerna
mars 2023

Räddningstjänsten Syd

Granskning av IT-säkerhet och informationssäkerhet

Building a better working world

Innehåll

1. Sammanfattning

Granskningens övergripande syfte är att bedöma hur direktionen säkerställer förbundets arbete med IT- och informationssäkerhet. Inom ramen för granskningen har vi bedömt ett antal olika kontrollpunkter fördelade på de olika momenten kontrollmiljö, riskanalys, kontrollaktiviteter, information/kommunikation och utvärdering/uppföljning. Resultatet av granskningen visar följande fördelning.

Sammanfattande tabell, kontrollpunkter;

	Kontrollen finns och fungerar tillfredsställande.	Kontrollen finns och fungerar delvis.	Kontrollen finns ej eller fungerar ej tillfredsställande.
Kontrollmiljö	3	3	0
Riskanalys	2	3	2
Kontrollåtgärd	24	11	1
Information/kom.	2	0	0
Uppföljning/utvärdering	3	4	0

Vår bedömning är att direktionen behöver stärka IT- och informationssäkerheten inom förbundet. Det finns enligt vår bedömning en god grund avseende organisation och förutsättningar. Trots detta menar vi att det på ett fåtal punkter saknas tillfredsställande förutsättningar, och på ett flertal att förutsättningarna inte är fullgoda. Vi lämnar mot bakgrund av granskningen ett stort antal rekommendationer. Flera av dessa syftar till att dokumentera och systematisera arbetssätt och rutiner.

Vi rekommenderar direktionen att

- Stärka möjligheten till direkt återrapportering avseende IT- och informationssäkerhetsarbetet.
- Klassa informationstillgångar i enlighet med sekretess, riktighet och tillgänglighet.
- Reglera förutsättningarna för utlämning av information till tredje part.
- Dokumentera samtliga informationssystem i en systemförteckning.
- Förteckna ansvarsfördelning avseende förbundets samtliga informationstillgångar.
- Upprätta dokumenterade systemsäkerhetsanalyser för samtliga informationssystem.
- I avtal reglera vem som har informationssäkerhetsansvaret för drift som förlagts på utomstående part.
- Dokumentera krav för externa konsulter med avseende på introduktion och utbildning för att verka i förbundets IT-miljö.
- Skapa rutiner för uppföljning och granskning av leverantörers tjänster. Detta för att säkerställa att avtal följs och att förbundets krav på externa parter efterlevs.
- Reglera hur tredje part får tillgång till förbundets information eller informationssystem.

- Stärka identitetskrav för upplåsning av användares konton, samt att inte dela ut tillfälliga lösenord över telefon.
- I kontinuitetsplan dokumentera de längsta acceptabla avbrottstiderna för kritiska IT- och informationssystem.
- I kontinuitetsplan dokumentera återstartsrutiner.
- Överväga genomföra externa penetrationstester.
- Systematisera och dokumentera den övergripande uppföljningen av säkerhetsrutiner och policys.

2. Inledning

2.1. Bakgrund

Idag bedrivs så gott som all verksamhet i förbundet med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet och antalet olika programvaror är stort. För att uppnå förbundets mål krävs att informationen i verksamhetsstödet är tillgänglig, riktig, har korrekt konfidentialitet samt är spårbar.

Den 25 maj 2018 ersatte den nya dataskyddsförordningen (GDPR) den svenska personuppgiftslagen. Det nya regelverket kan innebära stora förändringar för den kommunala verksamheten vilket gör det angeläget att utvärdera dess konsekvenser för förbundets verksamheter.

Mot bakgrund av genomförd risk- och väsentlighetsanalys önskar revisorerna granska förbundets arbete med intern kontroll av IT-säkerheten.

2.2. Syfte och avgränsning

Granskningens övergripande syfte är att granska hur effektivt Räddningstjänsten Syd arbetar med informationssäkerhet. Granskningen utgår från ett internkontrollperspektiv där granskningen sker av hur direktionen följer och leder arbetet med intern kontroll inom IT-säkerhetsområdet för att säkerställa att den interna kontrollen är tillräcklig.

Avgränsning

Granskningen genomförs genom insamling av bakgrundsinformation inför intervjuer. Relevant information är organisation, IT-säkerhetspolicy, riskanalyser, rapportering av kontrollaktiviteter, tidigare granskningsrapporter mm. Intervjuer med representanter från förbundets IT-organisation som arbetar med IT-och informationssäkerhet.

Områden för revisionell bedömning

I granskningen kommer följande huvudområden att följas upp:

- Kontrollmiljö
  - Säkerhetspolicy
  - Säkerhetsorganisation
- Riskanalys
  - Vilka riskanalyser av IT-säkerheten genomförs
- Kontrollåtgärd
  - Klassificering och kontroll av tillgångar
  - Personal och säkerhet
  - Fysisk och miljörelaterad säkerhet
  - Styrning av åtkomst
  - Styrning och kommunikation av drift
- Information och kommunikation
  - Incidenthantering
- Uppföljning och utvärdering
  - Systemutveckling och underhåll
  - Kontinuitetsplanering

- Efterlevnad

2.3. Revisionskriterier

COSO-modellens ramverk för intern kontroll utgör grundkriterierna för granskningen. Vidare genomförs granskningen mot så kallad god praxis inom informationssäkerhetsområdet genom utvalda delar av Myndigheten för samhällsskydd och beredskaps ramverk för IT- och informationssäkerhet BITS (Basnivå för IT-säkerhet), som är ett etablerat ramverk i ett stort antal kommuner eller kommunal verksamhet och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27001.

Ansvarig nämnd
Granskningen avser direktionen.

2.4. Metod

Granskningen har genomförts genom insamling av bakgrundsinformation inför intervjuer. Relevant information är organisation, IT-säkerhetspolicy, riskanalyser, rapportering av kontrollaktiviteter, tidigare granskningsrapporter mm. Intervjuer med representanter från förbundets IT-organisation som arbetar med IT-och informationssäkerhet.

Utifrån insamlat material har en bedömning gjorts av förbundets IT-säkerhets- och informationssäkerhetsarbete.

Intervjuade har beretts tillfälle att faktagranska rapporten.

3. Revisionskriterier

3.1. Granskningsstruktur

Kontrollmiljön anger tonen i en organisation och påverkar kontrollmedvetenheten hos dess medarbetare. Faktorer som innefattas av kontrollmiljön är integritet, etiska värden, kompetensen hos medarbetarna i organisationen, ledningens filosofi och ledarstil, det sätt på vilket ledningen fördelar ansvar och befogenheter och organiserar och utvecklar dess medarbetare samt den uppmärksamhet och vägledning som ledningen ger.

Riskbedömning, vilket innebär identifiering, analys och hantering av relevanta risker för att uppnå organisationens mål och krav. Riskvärderingen bör alltid dokumenteras i syfte att förtydliga systematiken.

Kontrollaktiviteter är de riktlinjer och rutiner som bidrar till att säkerställa att brister upptäcks och att direktiv genomförs. De bidrar till att säkerställa att nödvändiga åtgärder vidtas för att hantera risker för att organisationens mål inte uppnås.

Information och kommunikation måste identifieras, fångas, och förmedlas i en sådan form och inom en sådan tidsram att de anställda kan utföra sina uppgifter.

Interna styr- och kontrollsystem behöver övervakas, följas upp och utvärderas – en process som bestämmer kvaliteten på systemets resultat över tid. Det åstadkoms genom löpande övervakningsåtgärder och uppföljningar, separata utvärderingar eller en kombination av dessa.

3.2. Myndigheten för samhällsskydd och beredskaps ramverk för IT-säkerhet, BITS

Begreppet informationssäkerhet omfattar IT-säkerhet och administrativ säkerhet. IT-säkerhet är skydd av information i informationsbehandlande tekniska system. Administrativ säkerhet avser regler för personal och säkerhetsklassning av information. Informationssäkerhet innebär att tillgänglighet, riktighet, konfidentialitet och spårbarhet säkerställs. För att kunna säkerställa en tillräcklig nivå av informationssäkerhet är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt.

Myndigheten för samhällsskydd och beredskap (MSB) har utarbetat ett ramverk som utgör en basnivå för informationssäkerhet. EY har utifrån detta ramverk och erfarenheter från tidigare granskningar inom området valt ut följande aspekter att fokusera på: säkerhetspolicy, organisation, riskanalyser av IT-säkerheten, klassificering och kontroll av tillgångar, personal och säkerhet, fysisk och miljörelaterad säkerhet, styrning av åtkomst och kommunikation av drift, incidenthantering, systemutveckling och underhåll samt kontinuitetsplanering.

4. Granskningsresultat

Rapporten redovisar i vilken grad förbundet uppfyller valda rekommendationer ur BITS. Resultatet är en sammanvägd bedömning, som baseras på information som lämnats vid intervjuerna samt genom erhållen dokumentation. Den sammanvägda bedömningen av svaren på kontrollerna har bedömts enligt följande alternativ:

Ja	Kontrollen finns och fungerar tillfredsställande.
Delvis	Kontrollen finns och fungerar delvis.
Nej	Kontrollen finns ej eller fungerar ej tillfredsställande.
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl.

4.1. Kontrollmiljö

I kontrollmiljön ingår moment som kan hänföras till ledningsfrågor, organisation, riktlinjer och styrdokument samt resursfrågor. Kontrollmiljön inbegriper ofta målformuleringar eller andra krav som ställs på verksamheten, därför är bedömning av riktlinjer av särskilt intresse. Även personalens kompetens och de insatser som genomförs som vidareutbildning m.m. ingår i kontrollmiljön. Kontrollmiljön är viktig för att bedöma förbundets förmåga att leda verksamheten i riktning mot säkerhet i och i anslutning till informationssäkerhetssystemen.

IK 1 Organisation av säkerheten, policy m.m.			
1.1	Finns policy och riktlinjer för informationssäkerhet?	Förbundet har en beslutad (2022-09-05) IT-riktlinje för Räddningstjänsten Syd. Syftet är för anställda och förtroendevalda att skapa en tydlig struktur över hur IT ska hanteras och användas i organisationen. Den ska öka kunskapen kring IT, effektivisera informationsflödet och användandet samt att öka säkerheten i verksamheten.	
1.2	Beskriv organisation, kompetens och behov	Organisationen för IT- och informationssäkerhet är uppdelad i två områden; IT och radio. Det finns en systemansvarig samt två tekniker som arbetar med IT-frågor. Därtill finns en extern konsult som är inhyrd för flertalet uppgifter, bland annat serverstruktur. Supportfunktioner är kopplade till IT-området. Det framförs att organisationen skulle behöva stärkas ytterligare. Det saknas sedan 2017 en renodlad IT-chef. IT-funktionerna är i dagsläget organiserade under funktionschefen för Teknik. Däri ingår flera andra funktioner vilket innebär ett bredare fokus. Förbundets IT-organisation är inte en delad funktion med någon av medlemskommunerna. Däremot kan förbundet använda sig av Malmö Stads tjänsteutbud.	

1.3	Finns det en informationssäkerhetssamordnare eller motsvarande?	Ja. Enhetschef för verksamhetsstöd är tillika informationssäkerhetssamordnare.	
1.4	Har organisationen utsett systemägare för samtliga informationssystem?	Ja. Det finns ett flertal systemägare för systemen. Ägandeskapet är kopplat till medarbetare med ansvar för arbetsuppgifter kopplat till systemen. Exempelvis är controller systemägare för ekonomisystem, och HR-chefen systemägare till HR-systemet. Enhetschef för verksamhetsstöd har det övergripande ansvaret.	
1.5	Finns det en samordningsfunktion för att länka samman den operativa verksamheten för informationssäkerhet och ledningen?	Ja. Enhetschef för verksamhetsstöd ingår i ledningsgruppen. IT- och informationssäkerhetsfrågor lyfts av enhetschef till ledningsgrupp när det finns behov för det. Det framförs exempel vid intervju. Enhetschefen har däremot inte informerat vid direktionens sammanträde. Det framförs att sådana frågor i så fall lyfts vidare från förbundsdirektören.	
1.6	Har ansvaret för informationssäkerheten reglerats i avtal i de fall verksamhet/drift m.m. lagts ut på en utomstående organisation?	Det regleras i avtal hur externa parter får använda information som kommer från förbundet. Det har dock enligt uppgift inte reglerats vem som ansvarar för informationssäkerheten. Det framhålls att förbundet är aktiva i fall då de fått information om eventualiteter som kan ha påverkan på informationssäkerheten. Detta exemplifieras med extern part som ville övergå till Amazons serverlösningar. Detta nekades med motivering att det inte kunde garanteras att informationstillgångar lagras inom EU. Det framförs att majoriteten av informationstillgångar som avser verksamhetssystem är placerade på egna servrar.	

4.2. Riskanalys

I riskanalysen ingår att bedöma hur förbundet arbetar med IT-säkerheten utifrån riskanalys och identifiering av olika risker. Riskanalysen bör vara utformad med vedertagna metoder om sannolikhet och konsekvenser. Riskanalysen bör också vara genomförd av medarbetare/personer som besitter tillräcklig kompetens för att identifiera och bedöma risker. Handlingsplaner bör vara kopplade till risker som har höga riskvärden.

IK 2 Riskanalys			
2.1	Genomförs riskanalyser avseende IT- och informationssäkerhet?	Det har genomförts en säkerhetsskyddsanalys. Denna omfattar analys av risker kopplade till IT- och informationssäkerhet. Det genomförs säkerhetsanalyser löpande om det skulle uppstå specifika situationer som inte omfattas av säkerhetsskyddsanalysen. Systematiken i arbetet är att löpande värdera risker för verksamheten. Det finns ingen rutin för årlig utvärdering eller riskinventering.	
2.2	Har verksamhetskritiska IT-system identifierats och bedömts?	Ja, i kontinuitetshanteringsplan. Detta ligger inom ramen för total- och civilförsvar. Förbundets verksamhet ska vara möjlig att upprätthålla även vid verksamhetspåverkande händelser. Inom ramen för denna bedömning har verksamhetskritiska IT-system identifierats och utvärderats. Detta omfattar hela verksamheten och är inte isolerat till IT- och informationssäkerhet. Som del av kontinuitetsplaneringen genomförs kontinuerliga back-up av system, eller delar av system, som är kritiska för verksamheten.	
2.3	Har omständigheter som ska betecknas som kris/katastrof (extraordinära händelser) för verksamheten kartlagts?	Ja. Det framförs finnas en bred planering för händelser som är att beteckna som extraordinära. En grundinställning är att förbundet ensamt ska kunna hantera samtliga händelser utan att förlita sig på externa parter. Samtliga beroenden är identifierade och kartlagda. Dessa kartläggningar omfattas av sekretess och förvaras säkert.	
Klassificering och kontroll av tillgångar			
2.4	Är organisationens information klassad avseende sekretess/riktighet/tillgänglighet (har systemägarna yttrat sig om klassning)?	Ja. Det har dock inte nödvändigtvis att göra med säkerhetsskydd. Det kan vara hänförligt till personalärenden varpå sekretessklassificering behöver göras av andra anledningar. Det framhålls att förbundet är en offentlig verksamhet som följer de regler som är tillämplig. En klassning sker automatiskt genom utlämnande enligt offentlighets- och sekretesslagstiftningen. Samtliga utlämnande av information föregås av en bedömning. Kansliet är den enda organisatoriska delen av förbundet som kan lämna ut uppgifter. När det kommer till tillgänglighet kan inte vem som helst se allt. Detta avser exempelvis Daildalos som	

		är ett verksamhetssystem som tillämpas inom förbundet. Informationen i systemet är behörighetsstyrd på intranätet och filservern. Det saknas dock enligt uppgift från intervju en standardisering eller av riktlinjer tydliggjorda rutiner för hantering av klassning.	
2.5	Har samtliga informationssystem identifierats och dokumenterats i en aktuell systemförteckning?	Nej, det saknas en systemförteckning över samtliga system. Det saknas också en samlad förteckning över systemägare. Det framförs att det finns en ambition att upprätta en systemförteckning.	
2.6	Finns det en ansvarsfördelning för organisationens samtliga informationstillgångar?	Det saknas en förtecknad ansvarsfördelning för förbundets samtliga informationstillgångar. Det framförs att ansvaret inom organisationen anses följa verksamhetscheferna. Det är dock otydligt om detta är uttalat. Det finns ett dokument som avser hantering av personuppgifter. Direktionen är enligt dokumentet personuppgiftsansvarig. Direktionen har delegation på dataskyddsombud.	

4.3. Kontrollåtgärder

Kontrollåtgärder är olika insatser som genomförs för att minska riskerna i verksamheten och bidra till en ökad intern kontroll av processerna. De moment som vi bedömer under detta avsnitt är: personal och säkerhet, fysisk och miljörelaterad säkerhet, styrning av kommunikation och drift, styrning av åtkomst samt anskaffning, utveckling och underhåll av informationssystem. Kontrollsystemen bidrar till att säkerställa IT-systemen är tillgängliga för rätt person i rätt tid och på ett spårbart sätt.

IK 3 Personal och säkerhet			
3.1	Får inhyrd/inlånad personal information om vilka säkerhetskrav och instruktioner som gäller? (utbildning/ introduktion/kurs m.m.)	Förbundet använder sig i huvudsak av samma konsulter återkommande. Det uppges vara ovanligt att det är nya konsulter som hyrs in. Det uppges att samtliga får information om vilka regler som gäller på förbundet. Om konsulter kommer att vara inhyrda en längre tid görs en säkerhetsklassning. Det framförs att avtalen med konsulter omfattar sekretessklausuler. Det saknas rutinbeskrivningar för kraven på inhyrda konsulter. Det finns ej heller krav på utbildning av nya konsulter.	

3.2	Har systemägaren definierat vilka krav som ställs på användare som får tillgång till informationssystem och information (leta information i individuella akter m.m.)?	Ja, detta lyfts i riktlinje för IT. Dessutom genomgår nyanställda utbildning. Det uppges att förbundets anställda vet vilka krav som gäller. Grundläget är att anställda inte ska leta information som inte har med ens arbetsuppgifter att göra.	
3.3	Genomförs regelbundet utbildningsinsatser inom informationssäkerhet?	På medarbetardagarna hade de information om IT-säkerhet. De har även information kring säkerhetsskyddet som man får när man är nyanställd. Har även utbildning om nätfiske genom till exempel 10 minuters utbildningar. Små moment ”såhär känner du igen nätfiske”, för att stoppa phishing. Max en gång varje vecka genomförs utbildningsinsatser. Förbundet skickar regelbundet ut mail för att kontrollera att folk har förstått informationen de tagit del av. Om man upptäckt phishing mail ska man kontakta supporten, har de anställda lärt sig. Men till slut blir folk så vana vid det så att de inte längre hör av sig.	
3.4	Dras åtkomsträtten till information och informationsbehandlingsresurser in vid avslutande av anställning eller vid förflyttning?	Ja. Det görs genom AD (ett användarregister som styr åtkomster och rättigheter på ett nätverk). När anställda byter befattning förändras åtkomsträtten genom AD. Tidigare kunde man komma åt intranätet även om man slutat. Dock inte tillgångarna på intranätet.	
3.5	Finns funktioner för att förhindra obehörigt fysisk tillträde till organisationens lokaler och information?	Ja, nyckeltaggar på samtliga dörrar. För två år sedan strukturerade förbundet om tillträde till lokalerna. Åtkomst till lokaler finns dokumenterat.	
3.6	Har IT-utrustning som kräver avbrottsfri kraft identifierats?	Ja. Detta utgör en del av kontinuitetsplanen.	
3.7	Finns larm kopplat till larmmottagare för: - Brand, temperatur, fukt? - Sker test av larmmottagare?	Ja.	
3.8	Finns i direkt anslutning till viktig datorkommunikationsutrustning en kolsyresläckare?	Ja. Det finns både bärbar och installerad släckutrustning.	

3.9	Raderas känslig information på ett säkert sätt från utrustning som tas ur bruk eller återanvänds? (omformatering, raderingsprogram m.m.)	Ja, alla datorer och servrar som innehåller möjlighet till lagring formateras på ett säkert sätt. Standardrutiner finns för att radera känslig information.	
3.10	Finns särskilda säkerhetsåtgärder för utrustning utanför ordinarie arbetsplats?	Ja. Anställda har enligt IT-riktlinje möjlighet att använda utrustning utanför ordinarie arbetsplats. De har spärrar för att nyttja utrustning utanför norden och Tyskland. Inloggning från annan plats än arbetsplats kräver tvåfaktorsinloggning. Detta sker genom VPN-tunnel (krypterad kanal).	
3.11	Finns information och regler som anger att IT-utrustning m.m. inte får föras ut från organisationens lokaler utan medgivande från ansvarig chef?	Ja. Detta är definierat i IT-riktlinjerna. Det krävs inga formella tillstånd. Får du en bärbar dator får du information om hur du får använda utrustningen.	
3.12	Finns driftdokumentation för verksamhetskritiska informationssystem? (backup, jourpärm m. kontaktpersoner)	Delvis. Det finns spårbarhet på en stor del av systemen. Dock inte på samtliga plattformar. Kontaktpersoner för de kritiska verksamhetssystemen är inkluderat i kontinuitetsplanen. Backup sparas för de kritiska systemen. Förbundet har möjlighet att återställa system till det senaste fungerade tidpunkten. Det finns tre backuper placerade på två fysiska platser.	
3.13	Sker system-/programutveckling samt tester av modifierade system åtskilt från driftsmiljön?	I huvudsak ja. Det beror på system. I huvudsak sköts detta av de externa systemleverantörerna. Dessa testar exempelvis uppdateringar utanför förbundets system innan det implementeras på plats. Vid introducering av nya verktyg och system görs detta enligt uppgift alltid separerat från driftsmiljön.	
3.14	Finns rutiner för hur utomstående leverantörers tjänster följs upp och granskas?	Det saknas specifika rutiner för hur utomstående leverantörers tjänster ska följas upp och granskas. Detta kan regleras i avtal med leverantör. Det skiljer sig dock från fall till fall hur uppföljningen ser ut. I grund och botten genomförs uppföljningar först om något inte fungerat som det ska.	

3.15	Godkänner systemägaren eller annan lämplig personal driftsättningar av förändrade informationssystem?	Ja, i största möjliga utsträckning. Enhetschefen för verksamhetsstöd hanterar inte det tekniska men kan ta beslut i vissa fall. Systemägarna är delaktiga i implementeringsfasen. Inköp godkänns genom attestering.	
3.16	Finns det för både servrar och klienter rutiner för skydd mot skadlig programkod?	Ja. Brandväggar och antimalware-programvara (på såväl klienter som servrar).	
3.17	Har organisationens nätverk delats upp i mindre enheter (segmentering) så att en (virus-) attack enbart drabbar en del av nätverket?	Ja.	
3.18	Genomförs säkerhetskopiering regelbundet?	Ja.	
3.19	Saknas det alternativa vägar vid sidan av organisationens brandvägg in till det interna nätverket?	Ja. Det skulle krävas fysiskt tillträde till servrar.	
3.20	Finns det dokumenterade regler avseende vilken information som får skickas utanför organisationen? (ex sekretessbelagd info)	Delvis. Samtlig utlämnande av information ska göras av kansliet. Dessa gör bedömning huruvida informationen kan ges ut eller ej. Detta är dock inte reglerat i riktlinjer.	
3.21	Sparas revisionsloggar för säkerhetsrelevanta händelser?	Delvis. Det uppges att loggar sparas för majoriteten av systemen. Det finns dock differenser i hur länge loggar sparas. Vissa system är lagringen kortsiktig. Förbundet har inga specificerade krav på hur lång tid loggar ska sparas av systemen. Vid incidenter sparas loggar ner för längre förvaring.	
Styrning av åtkomst			
3.22	Har organisationen satt upp dokumenterade regler för åtkomst/tillträde för tredje parts åtkomst till information eller informationssystem?	Det finns inga specificerade eller standardiserade regler för tredje parts åtkomst. Det framförs att de leverantörer som har tillgång till exempelvis, och i huvudsak, verksamhetssystemet Daedalos regleras i avtal.	
3.23	Tilldelas användare en behörighetsprofil som endast medger åtkomst till de system som krävs för arbetsuppgiften?	Ja. Detta styrs i huvudsak av AD-registret.	
3.24	Begränsas rätten att installera nya program i nätverket samt den egna arbetsstationen till	Ja. Det kan som mest installeras skrivarrutiner på medarbetares datorer. På mobiltelefoner är anställda fria att installera appar. Telefonerna är dock	

	endast utsedd behörig personal?	inte per automatik inloggade på förbundets nätverk. Ett fåtal appar har tillgång till interna informationstillgångar, och då genom krypterade former. Exempelvis mail-appar.	
3.25	Har samtliga administratörer fullständiga systembehörigheter eller endast vad som krävs för att fullgöra arbetsuppgiften?	Administratörer har begränsningar kopplade till arbetsuppgifterna. Vissa administratörer har bredare behörighet än så. Detta för att säkerställa en redundans vid sjukfrånvaro, semestrar och dylikt. Det finns inga ”superusers” på administratörsnivå.	
3.26	Genomförs kontinuerligt (minst en gång per år) kontroll av behörigheterna i organisationen?	Det är beroende på vilket system som avses. För verksamhetssystemet Daedalos görs behörighetskontroll en gång i halvåret. Det görs årliga kontroller av taggar. Kontroll sker av taggar som inte använts under de senaste tre månaderna. Det finns inte en systematisk kontroll av samtliga behörigheter för samtliga system. Det görs vid tillfällen stickprovskontroller. Som mest framkommer att enstaka medarbetare haft behörighet som överstiger kraven för arbetsuppgift, vanligtvis på grund av byte av tjänst. Det saknas dokumenterade rutiner för det övergripande arbetet med behörighetskontroller inom förbundet. Oaktat om detta ska göras genom stickprovskontroller eller ej.	
3.27	Öppnas låsta användarkonton endast efter säker identifiering av användaren?	Det framförs att detta görs baserat på resurserna de har. Det tillämpas inga säkra tjänster för validering av identitet (exempelvis Bank-ID). Om supportfunktionen skulle vara osäkra eller att det handlar om känsliga behörigheter görs kontroller, så som fysik identifiering. Men det krävs i normalfallet inte att medarbetare behöver begära upplåsning genom ett fysiskt besök. Det betonas att det är en liten organisation där medarbetarkännedomen är hög. Tillfälliga lösenord lämnas över telefon eller vid fysiskt besök. De försöker att undvika att skicka lösenord i mail.	
3.28	Finns en gemensam lösenordspolicy?	Delvis. Det finns inte en gemensam lösenordspolicy. Detta definieras dock av de olika verksamhetssystemen, exempelvis Windows för 365-miljön. 365-miljön tillåter dock inte en-lösenordsaccess till andra system så som Daedalos. Detta system har också krav på komplexitet.	
3.29	Finns en dokumenterad brandväggspolicy där det beskrivs	I huvudsak ja. Detta är dokumenterat i brandväggen. Den huvudsakliga policyn är att allt är blockerat *in* i brandväggen, och att ta *ut* information styrs	

	vilka tjänster brandväggen ska tillhandahålla?	av användarrättigheter. Det finns därtill skydd gentemot vissa typer av hemsidor. Förbundet har nyligen genomfört en övergång i servermiljön. Den tidigare miljöns regelverk uppges ha varit väldigt komplicerat.	
3.30	Har organisationen ställt och dokumenterat tekniska säkerhetskrav och krav på praktisk hantering avseende användandet av mobil datorutrustning och distansarbete?	Ja.	
3.31	Finns det aktuell dokumentation med regler för distansarbete?	Ja.	
Anskaffning, utveckling och underhåll av informationssystem			
3.32	Har en systemsäkerhetsanalys upprättats och dokumenterats för varje informationssystem som bedöms som viktiga?	Nej. Det framförs att systematiken är att system som införs gör för att innefatta en viss typ av information. Det genomförs översyner av vilken typ av information som ska finnas i systemen. Exempelvis krigsplaceringar i HR-systemet. Men en regelrätt systemsäkerhetsanalys dokumenteras inte systematiskt för varje informationssystem av vikt.	
3.33	Krypteras persondata som förmedlas över öppna nät?	Ja. Majoriteten av persondatan är krypterad. Det saknas dock kryptering för epost. Dock framförs att det inte är vanligt att de hanterar persondata över epost. Lönebesked lämnas via Kivra som har kryptering. Ärenden från HR-systemet förmedlas inte i annat fall heller ut från systemet. Medarbetare får ett meddelande om att de har ett meddelande att läsa i systemet. Utskrifter är krypterade mellan klient och skrivare.	
3.34	Finns det utsedd personal som ansvarar för systemunderhåll (angivna personer per system?)	Ja.	
3.35	Finns det regler och rutiner för hur system- och programutveckling ska genomföras?	Det saknas dokumenterade regler. Rutinen är att involvera IT-avdelningen. Det meddelas exempelvis centralt till samtliga berörda om uppdateringar kräver att system är otillgängliga.	
3.36	Finns det en uppdaterad och aktuell systemdokumentation för informationssystemen?	Det finns för de stora informationssystemen tillhörande systemdokumentation, exempelvis ”wiki” där systemdokumentation förs in och uppdateras. Förbundet har ingen egen yta där samtlig systemdokumentation sparas.	

4.4. Information och kommunikation

Det är av stor vikt att medarbetare vet var de ska vända sig eller hur de ska agera vid olika situationer. Hantering av informationssäkerhetsincidenter ingår därför som en del av informations- och kommunikationskanalerna genom att medarbetare ska ha just den informationen om störningar m.m. i systemen uppstår.

IK 4 Hantering av informationssäkerhetsincidenter			
4.1	Finns det dokumenterade instruktioner avseende vart användare skall vända sig och hur de ska agera vid funktionsfel, misstanke om intrång eller vid andra störningar?	Ja. Medarbetare ska vända sig till supporten.	
4.2	Har medarbetarna kunskap om vart de ska vända sig?	Ja. Det finns en gemensam kanal in, men det händer att användare vänder sig till specifika tjänstemän på IT.	

4.5. Uppföljning och utvärdering

Som utvärdering bedöms kontinuitetsplanering i verksamheten samt efterlevnaden. Det vill säga hur verksamheten upprätthålls vid avbrott eller störningar.

IK 5 Kontinuitetsplanering i verksamheten			
5.1	Finns det en gemensam kontinuitetsplan dokumenterad för organisationen?	Ja. Denna är dokumenterad och förvaras säkert.	
5.2	Har systemägaren eller motsvarande beslutat om den längsta acceptabla tid som informationssystemet bedöms kunna vara ur funktion innan verksamheten äventyras?	Delvis. Det är enligt uppgift inte beslutat som del av kontinuitetsplanen. Däremot finns det definierat i flertalet avtal med respektive systemleverantör.	
5.3	Finns det en dokumenterad avbrottsplan med återstarts- och reservrutiner för datadriften som vidtas inom ramen för den ordinarie driften?	Det framförs att det finns kunskap för reservrutiner för datadriften och kunskap om återstartsrutiner. Det finns viss redundans där servrar automatiskt flyttar över till en annan vid avbrott. Även andra system är möjliga att hantera även vid avbrott. Detta är dock inte dokumenterat.	
Efterlevnad			
5.4	Används endast programvaror i enlighet med gällande avtal och licensregler?	Ja. Det finns lite utrymme att göra avsteg från licensreglerna.	
5.5	Har organisationen förtecknat och anmält personuppgifter till personuppgiftsombud?	Ja.	

5.6	Genomförs interna och externa penetrationstester kontinuerligt?	Delvis. Det genomförs phishing-tester för att säkerställa efterlevnad mot så kallad ”social-engineering”. Det genomförs inga penetrationstester genom exempelvis simulerade hacker-attacker. Det framförs att de med jämna mellanrum blir utsatta för intrångsförsök från okända aktörer. Så kallade dörrknackningar.	
5.7	Granskar ledningspersoner regelbundet att säkerhetsrutiner, policy och normer efterlevs?	Enligt uppgift görs detta kontinuerligt. Detta görs till del i en aktiv miljö. Detta genom att kontrollen sker i vardagen, genom att säkerställa att anställda agerar i enlighet med rutiner och regler. Det finns inga dokumenterade regler med intervall eller specificerade moment för att säkerställa dess efterlevnad.	

5. Analys avseende intern kontroll

Inom ramen för granskningen har vi bedömt ett antal olika kontrollpunkter fördelade på olika moment inom intern kontroll. Resultatet av granskningen visar följande fördelning.

Sammanfattande tabell, kontrollpunkter

	Kontrollen finns och fungerar tillfreds-ställande.	Kontrollen finns och fungerar delvis.	Kontrollen finns ej eller fungerar ej till-fredsställande.
Kontrollmiljö	3	3	0
Riskanalys	2	3	2
Kontrollåtgärd	24	11	1
Information/kom.	2	0	0
Uppföljning/utvärdering	3	4	0

Vår bedömning är att direktionen behöver stärka IT- och informationssäkerheten inom förbundet. Det finns enligt vår bedömning en god grund avseende organisation och förutsättningar. Trots detta menar vi att det på ett fåtal punkter saknas tillfredsställande förutsättningar, och på ett flertal att förutsättningarna inte är fullgoda. Vi lämnar mot bakgrund av granskningen ett stort antal rekommendationer. Flera av dessa syftar till att dokumentera och systematisera arbetssätt och rutiner.

Kontrollmiljö
Det finns en IT-riktlinje för Räddningstjänsten Syd. Syftet med riktlinjen är att skapa tydlighet kring hur IT-utrustning och tjänster ska nyttjas. Det finns ur organisationen utsedd informationssäkerhetssamordnare. Likaså finns systemägare utsedda. Det framgår av granskningen att det finns ett behov av stärkt organisation. Exempelvis saknas det en renodlad IT-chef inom organisationen.

IT är organiserat under funktionschefen för Teknik. Funktionen Teknik har ett bredare ansvar än endast IT. Rapportering av frågor rörande IT- och informationssäkerhet till ledningsgruppen görs av enhetschef för verksamhetsstöd. Rapportering till direktionen förs dock vidare av räddningschefen. Vi menar att det bör finnas mer direkta vägar för den operativa verksamheten att rapportera till direktionen.

Riskanalys
Förbundet har upprättat en säkerhetsskyddsanalys vilken inkluderar IT- och informationssäkerhetsrisker. Det saknas dock systematik för dess utvärdering och årlig riskinventering.

Det finns kontinuitetsplaner upprättade för hela förbundets verksamhet. Det är noterbart att det saknas standardiserade, eller på annat reglerat sätt, klassningar av information kopplat till sekretess/riktighet/tillgänglighet.

Det saknas förteckningar för förbundets samtliga informationssystem. Likaså saknas förteckning avseende ansvarsfördelning för förbundets informationstillgångar. Detta menar vi är angeläget att åtgärda. Personuppgiftsbiträde är utsett inom organisationen.

Kontrollåtgärder

Det finns ett flertal kontrollåtgärder på plats för att säkerställa en god driftmiljö. Dock finns också ett flertal områden där åtgärder bör vidtas för att stärka kontrollmiljön. Trots att förbundet inte nyttjar externa konsulter i bred mening menar vi att det bör säkerställas att det finns rutinbeskrivningar för säkerhetskrav, instruktioner och utbildning innan dess att de anlitas. Därtill saknas det rutiner för hur utomstående leverantörers tjänster systematiskt ska följas upp. Det är enligt vår mening inte tillräckligt att uppföljning främst görs först när system inte fungerar som de ska. Vi menar också att direktionen bör reglera hur tredje part får åtkomst till information- och/eller informationssystem.

Det är vidare vår bedömning att direktionen bör säkerställa att det regleras vilken typ av information som får utlämnas från förbundet. Det är positivt att endast kansliet ska kunna lämna ut information till extern part, vi kan dock inte se att det är reglerat att så är fallet.

Vi vill vidare poängtera vikten av att låsta konton endast öppnas efter säker identifiering av användaren. Likaså att tillfälliga lösenord inte lämnas ut över telefon.

Därtill menar vi att systemsäkerhetsanalyser bör upprättas och dokumenteras för varje informationssystem som bedöms som viktiga. Detta särskilt mot bakgrund av den känsliga natur som flera av informationstillgångarna omfattas av.

Avslutningsvis menar vi att det bör finnas regelverk som definierar rutiner för system- och programutveckling.

Information och kommunikation

Riktlinjerna för IT informerar om var man ska vända sig vid funktionsfel, misstanke om intrång eller störningar. Vi bedömer att detta är tillräckligt.

Uppföljning och utvärdering

Det finns enligt uppgift en omfattande kontinuitetsplan för förbundet. Det saknas dock information om längsta acceptabla avbrottstid i kontinuitetsplanen. För de system där avtal reglerar längsta acceptabla avbrottstid bör motsvarande information inkluderas i kontinuitetsplanen. Därtill bör återstarts- och reservrutiner dokumenteras. Detta för att motverka personbunden kunskap. Det är positivt att det återkommande genomförs så kallade ”phishing-tester”. Dessa kan med fördel kompletteras med penetrationstester.

Vi betvivlar inte att det sker en uppföljning av säkerhetsrutiner och policys, vi menar trots detta att detta arbete också bör systematiseras och dokumenteras för att säkerställa regelverkens efterlevnad.

Rekommendationer

Mot bakgrund av genomförd granskning rekommenderar vi direktionen att:

- Stärka möjligheten till direkt återrapportering avseende IT- och informationssäkerhetsarbetet.
- Klassa informationstillgångar i enlighet med sekretess, riktighet och tillgänglighet.
- Reglera förutsättningarna för utlämning av information till tredje part.
- Dokumentera samtliga informationssystem i en systemförteckning.

- Förteckna ansvarsfördelning avseende förbundets samtliga informationstillgångar.
- Upprätta dokumenterade systemsäkerhetsanalyser för samtliga informationssystem.
- I avtal reglera vem som har informationssäkerhetsansvaret för drift som förlagts på utomstående part.
- Dokumentera krav för externa konsulter med avseende på introduktion och utbildning för att verka i förbundets IT-miljö.
- Skapa rutiner för uppföljning och granskning av leverantörers tjänster. Detta för att säkerställa att avtal följs och att förbundets krav på externa parter efterlevs.
- Reglera hur tredje part får tillgång till förbundets information eller informationssystem.
- Stärka identitetskrav för upplåsning av användares konton, samt att inte dela ut tillfälliga lösenord över telefon.
- I kontinuitetsplan dokumentera de längsta acceptabla avbrottstiderna för kritiska IT- och informationssystem.
- I kontinuitetsplan dokumentera återstartsrutiner.
- Överväga genomföra externa penetrationstester.
- Systematisera och dokumentera den övergripande uppföljningen av säkerhetsrutiner och policys.

Malmö, den 7 mars 2023

Linus Aldefors
Certifierad kommunal yrkesrevisor
EY

Staffan Samuelsson
EY

Bilaga 1

Intervjuade funktioner

- Mikael Kess, funktionschef Teknik
- Johan Nilsson, IT-systemtekniker
- Markus Sjöstrand, Sambandsansvarig
- Glenn Bergbring, IT-konsult
- Joakim Blix, enhetschef Verksamhetsstöd