Revisionsrapport 2/2019
Genomförd på uppdrag av revisorerna
dec 2019-jan 2020

Storstockholms brandförsvar

Granskning av IT- och informationssäkerhet

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer

EY har på uppdrag av förbundets förtroendevalda revisorer genomfört en övergripande granskning av IT- och informationssäkerhet. Granskningen syftar till att bedöma om det föreligger en tillräcklig intern kontroll med avseende på förbundets arbete med IT- och informationssäkerhet.

Vår sammantagna bedömning är att förbundet inte fullt ut har säkerställt en tillräcklig intern kontroll med avseende på förbundets arbete med IT- och informationssäkerhet. Vår bedömning grundar sig på att ansvaret för informationssäkerhetsarbetet inte fullt är tydliggjort och att flera väsentliga policys och riktlinjer är under framtagande. Ett flertal åtgärder för att säkerställa en god intern kontroll har genomförts under året, bland annat riskanalyser, byte av IT-miljö och driftleverantörer samt framtagande av styrdokument. Däremot saknas en regelbunden rapportering till direktionen rörande verksamhetens IT- och informationssäkerhet. För svar på respektive revisionsfråga, se avsnitt 7 i rapporten.

Mot bakgrund av ovanstående rekommenderar vi direktionen att:

- Formalisera och tydliggöra uppdrag och roller vad gäller informationssäkerheten.
- Säkerställa att väsentliga policys och riktlinjer beslutas och förankras i organisationen
- Tydliggöra rutinerna mellan HR och IT-funktionen för när medarbetare slutar. Detta för att på ett ändamålsenligt sätt hantera information, konton och behörigheter.
- Säkerställa en ändamålsenlig uppföljning och återrapportering rörande IT- och informationssäkerhet.

2. Inledning

2.1. Bakgrund

Idag bedrivs så gott som all kommunal verksamhet med någon form av IT-stöd. IT-system har med tiden utvecklats till att bli en förutsättning för att kunna bedriva verksamhet. Antalet olika programvaror är stort och mängden ansamlad information i använda system är betydande. För att uppnå målen med verksamheten krävs att informationen som hanteras i bland annat verksamhetssystem är tillgänglig, riktig, har korrekt konfidentialitet[1] samt uppfyller krav på ändamålsenlig säkerhet.

Med utgångspunkt från riskanalys för 2019 har förbundets revisorer beslutat att genomföra en övergripande granskning av IT- och informationssäkerhet, med inriktning mot roller och ansvar, policys, riktlinjer samt hantering av säkerhetsfrågor.

2.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma huruvida det föreligger en tillräcklig intern kontroll med avseende på förbundets arbete med IT- och informationssäkerhet.

I granskningen har följande revisionsfrågor besvarats:

- På vilket sätt säkerställs informationssäkerhet samt funktionalitet och säkerhet i de IT-system som förbundet använder i sin verksamhet?
- Kan ansvarsfördelningen inom förbundet bedömas vara tydlig med avseende på IT- och informationssäkerhet?
- I vilken utsträckning kan fastställda styrdokument (policy, riktlinjer etc.) bedömas vara ändamålsenliga och följs efterlevnaden av dessa upp regelbundet av direktionen?
- I vilken utsträckning är de riskanalyser som upprättas inom förbundet, med avseende på IT- och informationssäkerhet, ändamålsenliga?
- I vilken utsträckning är återrapporteringen till direktionen avseende IT- och informationssäkerhet ändamålsenlig?
- I vilken omfattning används stöd från externa konsulter? Är uppföljning och utvärdering av externa tjänster ändamålsenlig i förekommande fall?

2.3. Genomförande

Granskningen grundas på intervjuer och dokumentstudier (se bilaga 1). Granskningen innebär inte att några säkerhetstester, penetrationstester eller dylikt av IT-system genomförs. Intervjuer har skett med ansvariga inom IT- och informationssäkerhet. Samtliga intervjuade har beretts tillfälle att sakgranska rapporten. Granskningen är genomförd december 2019-januari 2020.

[1] Med konfidentialitet avses att informationen inte får göras tillgänglig eller avslöjas för obehöriga.

3. Revisionella utgångspunkter

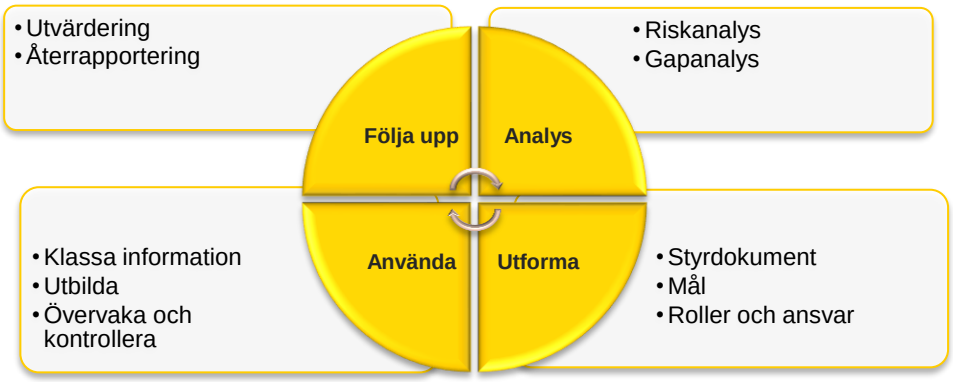
Granskningen har genomförts utifrån god praxis inom IT- och informationssäkerhetsområdet. Myndigheten för samhällsskydd och beredskap har tagit fram *Ledningssystem för informationssäkerhet*[2] (LIS) som är ett etablerat metodstöd och ramverk för informationssäkerhet inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27001. Nedan förklaras ramverket översiktligt.

3.1. Internationella standarder enligt ISO/IEC 27001

I verksamheters arbete med ledningssystem för informationssäkerhet finns det vissa standarder att beakta. De grundläggande standarderna har tagits fram inom ramen för samarbetet i de internationella standardiseringsorganen ISO[3] och IEC[4] och berör främst krav och riktlinjer för vilka säkerhetsåtgärder ledningssystemet generellt ska innehålla. I ISO 27001:2017 framgår att ledningen ska säkerställa att en informationssäkerhetspolicy och informationssäkerhetsmål är upprättade och integrerade i verksamhetsprocesser. Vidare bör det finnas en tydlig ansvarsfördelning med rapporteringsstruktur[5]. Standardserien har fokus på säkerhetsåtgärder men omfattar även frågor om styrning av informationssäkerhet såsom regelverk för informationssäkerhet (policy), organisation och efterlevnad.

3.2. Ledningssystem för informationssäkerhet – LIS

Metodstödet är uppdelat i fyra metodsteg med tillhörande metoddelar: identifiera och analysera, utforma, använda och följa upp.



Analysdelen inbegriper att kartlägga det nuvarande läget för informationssäkerhet, inklusive risker. MSB framhåller att ledningen bör se till att organisationen antar en policy med mål för informationssäkerhetsarbetet samt att roller och ansvar tydliggörs. I riktlinjer är det vanligt att det förs in bestämmelser om till exempel e-postanvändning, skydd mot skadlig kod, fysisk säkerhet, incidenthantering, kontinuitetsplanering, behörighetsadministration och loggning.

Användandet och genomförandedelen syftar på efterlevnaden av styrning och metodik. Incidenter, oförutsedda händelser och förändringar behöver hanteras. Medarbetare ska

[2] Myndigheten för samhällsskydd och beredskaps (MSB) definition av informationssäkerhet: Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
[3] International Organization for Standardization
[4] International Electrotechnical Commission
[5] MSB rekommenderar exempelvis att ett organisationsövergripande dokument klargör det mandat och den rapporteringsplikt som personen med ansvar för att leda och samordna informationssäkerhetsområdet har.

utbildas och klassningar ska genomföras och dokumenteras. Klassning är en förutsättning för att skapa rätt skydd för informationen.

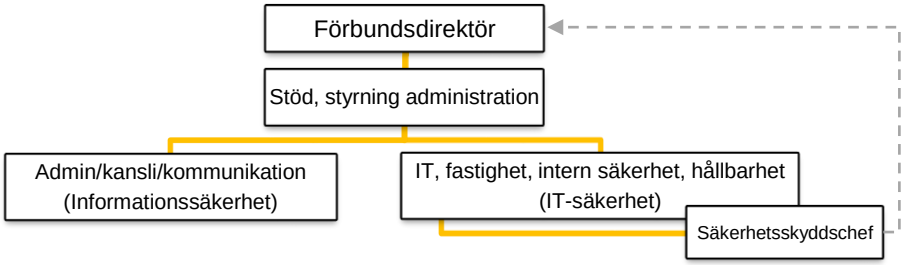
Resultatet från övervakning och mätningar av det systematiska informationssäkerhetsarbetet bör följas upp och återföras till förnyade analyser.

4. Styrning

4.1. Roll- och ansvarsfördelningen avseende IT- och informationssäkerhet

Samtliga policydokument fastställs av direktionen. Förbundsdirektören är ansvarig för säkerheten och den övergripande informationssäkerheten inom SSBF[6]. Säkerhetsarbetet leds av en säkerhetschef men varje verksamhetschef har ett lokalt ansvar[7]. Chefen för respektive verksamhet ansvarar för det lokala säkerhetsarbetet och att lagstiftning och interna styrdokument efterlevs.

Ansvaret för intern säkerhet och IT-säkerhet ligger på avdelningen för stöd, styrning och administration under enheten IT, fastighet, intern säkerhet, projekt och miljö. Enheten leds av en enhetschef och består av 15 medarbetare med befattningar som säkerhetschef, säkerhetsskyddschef och IT-strateg. Säkerhetskyddschefen rapporterar även direkt till förbundsdirektören avseende ansvaret säkerhetsskydd. Flera resursförstärkningar inom IT-organisationen inrättades 2017–2018.



IT-driftleverantörens servicedesk första linjen support för IT-frågor. Frågor som rör funktioner I verksamhetssystem skickas vidare till SSBF:s IT-enhet.

Det formella ansvaret för informationssäkerhet inom respektive verksamhet ligger enligt intervjuade på den avdelnings-/enhetschef som ansvarar för aktuell information. För närvarande är det kansliets arkivfunktion med cirka två medarbetare som arbetar med informationssäkerhetsområdet. Arbetet sker i nära samarbete med säkerhets- och säkerhetsskyddschef. En av arkivarierna har påbörjat en utbildning till informationssäkerhetsstrateg och beräknas vara färdig i maj 2020. Var kompetensen inom informationssäkerhet ska ligga organisatoriskt, är inte formellt definierat när granskningen genomförs. Enligt intervjuade finns ett behov av att formalisera uppdrag och rollbeskrivning för informationssäkerhetsfunktionen.

4.2. Styrdokument

I *Verksamhetsplan och budget 2019* har förbundet fått i uppdrag att:

[6] Policy för skydd och säkerhet
[7] Ibid

- Säkerställa att SSBF har ett ändamålsenligt säkerhetsskydd avseende informationssäkerhet, tillträdesbegränsning och säkerhetsprövning
- Skapa förutsättningar för samt stödja arbetet med ett systematiskt säkerhetsarbete på lokal nivå

Inom ramen för området skydd och säkerhet finns en övergripande policy och en riktlinje framtagna 2016 och uppdaterade 2019. Av policyn framgår förbundets övergripande mål och ansvarsfördelning kring säkerhetsområdet i sin helhet. Förbundet har även en beslutad riktlinje för arkivhantering. Förbundet saknar däremot en policy för informationssäkerhet. Enligt uppgift är denna under framtagande.

Härutöver finns följande flera riktlinjer som är under framtagande:

- Säkerhetsskydd[8]
  - Riktlinje, skydd av säkerhetskänslig verksamhet och säkerhetsklassade uppgifter (utkast för beslut)
- Säkerhet i kommunikationssystem[9]
  - Policy för skydd av kommunikationssystem (under framtagande)
  - Riktlinje för skydd av kommunikationssystem (under framtagande)
- Informationssäkerhet[10]
  - Riktlinje, hantering av sekretessreglerade uppgifter (under framtagande)
  - Riktlinje, hantering av hemliga uppgifter (under framtagande)

Vid tiden för granskningen är verksamheten i slutskedet att ta fram en ny riktlinje och policy för IT-användning och IT-säkerhet. Förbundsdirektören, ledningsgruppen och arbetstagarorganisationer har tagit del av och godkänt policy och riktlinje. Dokumenten tas upp till beslut i direktionen vid nästkommande direktionsmöte.

5. Informationssäkerhet samt funktionalitet och säkerhet i IT-systemen

5.1. Riskanalyser

Under 2018 och 2019 har det genomförts risk- och sårbarhetsanalyser på samtliga brandstationer avseende fysisk säkerhet, personalens säkerhet vid yrkesutövning, IT-säkerhet och samhällsviktig verksamhet. Riskanalyserna omfattas av sekretess och samtliga som deltar i riskanalysarbetet har enligt uppgift genomgått säkerhetsprövning.

I arbetet med att ta fram internkontrollplan för 2019 har riskanalys genomförts på förbundsnivå. Riskanalysen inbegriper riskkartläggning och sannolik- och väsentlighetsbedömning. Säkerhet med bäring på IT/informationssäkerhet finns med i internkontrollplanen. Risker gällande hantering av GDPR[11] bedöms höga och uppföljning av internkontrollplanen sker till direktionen i samband med årsbokslut.

[8] skydd av säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter
[9] skydd av system för IT, radiokommunikation och telefoni
[10] skydd av hemliga, sekretessreglerade och övriga känsliga uppgifter
[11] Dataskyddsförordningen (GDPR, The General Data Protection Regulation) gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras.

Risk- och sårbarhetsanalyser som genomförs utöver internkontrollarbetet vidrör informationsmängder av olika slag. När det gäller intern säkerhet avseende information genomfördes 2018 en kartläggning av samtliga arbetsprocesser där digital och analog information registrerades. En klassning av informationen väntas bli färdigställd under 2020.[12] Kartläggningen ska utgöra grunden för en informationshanteringsplan. Däremot finns inga regelrätta analyser genomförda med avseende på informationssäkerhet specifikt.

Förbundet har upphandlat konsulter för att analysera nivån på IT-säkerheten i SSBF:s IT-miljö. Analysen fokuserade på perimeterskyddets[13] kvalitet samt sårbarheter i servermiljön. Analysen resulterade i en direktupphandling av en IT-säkerhetsleverantör för att initialt komma tillrätta med bristerna som analysen visade. Detta har resulterat i en dokumenterad åtgärdslista för att höja IT-säkerheten. Däremot har inga penetrationstester genomförts.

5.2. Funktionalitet och säkerhet

Flera av förbundets verksamhetssystem används operativt kopplat till insats och ett antal verksamhetssystem är även integrerade med SOS Alarms system för att hantera larm-ärenden. På grund av de höga kraven på tillgänglighet och säkerhet används endast ett begränsat antal externa molntjänster. Verksamheten har därmed rådighet över kapacitet och tillgänglighet för verksamhetskritiska system. Vid systeminförande värderas bland annat tillgänglighet och robusthet.

För kommunikation mellan förbundets anläggningar hyrs redundant[14] fiber enbart avsedd för den egna verksamheten. Nuvarande brandväggslösning hanterar verksamhetskritisk trafik såsom utalarmering, ordinarie trafik, distansarbete och säker åtkomst för externa konsulter. Verksamheten har även säkerhetsdatorer placerade i skyddade säkerhetsskåp och en fristående skrivare för särskilda operativa ledningsfunktioner. Förbundets samtliga servrar är placerade i SSBF:s serverhall. Driften sköts av en upphandlad IT-driftleverantör. Enligt uppgift uppfyller serverhallen professionella krav vad gäller tillgänglighet, reservkapacitet och kyla. Serverhallen är tillträdesskyddad och kameraövervakad.

Flera åtgärder för att höja IT-säkerheten har genomförts under året, bland annat :

- Upphandling av ny IT-driftleverantör med högre leveranskrav
- Upphandling av en separat IT-säkerhetsleverantör
- Utbildning av chefer och annan personal kring IT- och informationssäkerhet
- Byte av brandväggslösning, kontinuerlig sårbarhetsskanning av servermiljön,
- Nya lösningar för extern tillgång för anställda samt externa leverantörer.
- Kontinuerliga möten med IT-säkerhetsleverantören.

Ytterligare mindre åtgärder för att säkerställa funktionalitet och säkerhet inbegriper:

- Ny lösenordspolicy (krav om 12 tecken). Till följd av detta har samtliga medarbetare tvingats ändra lösenord, vilket har stängt ute eventuella äldre inaktiva användare.
- Styrning av nyckelbrickor och elektroniska nycklar. När medarbetare avslutar sin anställning passiveras konton och nyckelbrickor.

[12] Klassificering av information är en grundläggande aktivitet för att information och resurser ska kunna ges nödvändigt skydd. Informationen ska klassificeras utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna, komma i orätta händer etc. De kriterier som tas upp i LIS är värde, legala krav, känslighet och betydelse för organisationens verksamhet. (MSB, Modell för klassificering av information)

[13] Säkerhetsfunktioner som skyddar egna tillgångar, exempelvis användare och nätverk, genom fysiska eller digitala väggar.

[14] En redundant förbindelse ska bestå av fysiskt separerade framföringsvägar

- I samband med serviceflytt och byte av IT-miljö[15] har användare inventerats, inklusive konsultkonton. Behörigheter och tillträde har begränsats och styrs mer strikt.

Intervjuade uppger att det finns ett behov av att stärka kommunikationen mellan förbundets HR-funktion och IT-funktion. Detta då informationen om att medarbetare har slutat inte rutinmässigt har förmedlats till IT. Intervjuade uppger att ett digitalt ärendehanteringssystem med möjlighet att logga ärenden av berörd art skulle underlätta.

Flera identifierade åtgärder återstår att genomföra. Utmaningarna rör bland annat äldre verksamhetssystem där det finns bindande avtal. En serverflytt är inplanerad 2020. Samtliga system kan dock inte bytas ut av budgetskäl och brist på personella resurser. Arbetet är påbörjat i form av upphandlingar och konkret utveckling av alternativa lösningar. Av handlingsprogrammet för åren 2016–2019[16] framgår att förbundet planerar att implementera ett digitalt ärende-, dokumenthanteringssystem samt e-arkiv. Detta har vid tiden för granskningen inte genomförts då upphandlingar av nya verksamhetssystem har prioriterats.

Eftersom flera informationsägare är externa parter utanför den egna organisationen har förbundet fört dialog och upprättat sekretessavtal med berörda informationsägare gällande den information som hanteras. SSBF rättar sig efter den informationsklassning som informationsägaren bedömt gäller. I några fall har förbundet återlämnat sekretessbelagd information till ägaren. Förbundet har tagit fram en teknisk lösning för hantering av sekretessklassad information. Riktlinje för hantering av hemliga uppgifter och sekretessreglerade uppgifter är under framtagande.

Våren 2018 upphandlades ett digitalt stöd för hantering av förbundets GDPR-arbete. Därutöver har förbundet initierat ytterligare åtgärder för att säkerställa följsamhet till dataskyddsförordningen, bland annat:

- Upphandling av juristfirma som upprätthåller rollen som dataskyddsombud inom förbundet.
- Översyn och upprättande av personbiträdesavtal med kunder och leverantörer där detta behövs.
- Registrering av förbundets personuppgiftsbehandling i olika verksamhetssystem.
- Kartläggning av personuppgifter i förbundets samtliga arbetsprocesser (pågår).

5.2.1. Avvikelsehantering

Verksamheten tillämpar ett webbaserat arbetsmiljöverktyg, (R)IA[17], för avvikelserapportering. Systemet är webbaserat och är gemensamt för räddningstjänsterna vilket främjar kunskapsspridning mellan organisationerna. Samtliga avvikelser som olycksfall, tillbud och säkerhetsavvikelser, inklusive de som rör IT- och informationssäkerhet, ska rapporteras i verktyget. Berörd chef ansvarar för riskvärdering och utredning.

Därutöver får IT-funktionen och IT-säkerhetsleverantören uppföljningar från IT-systemen. Som beslutsunderlag för analys och åtgärder används ett antal rapporter, bland annat trafik i brandvägg, sårbarheter i servermiljö och rapporter från virusskyddet. Dessa rapporter ger en helhetsbild av IT-säkerhetsnivån.

[15] Ny hårdvara samt senaste nivån på alla operativsystem som tillåter.
[16] Direktionen beslutade den 27 november 2019 att förlänga handlingsplanens giltighetstid till att även gälla 2020.
[17] IA är en förkortning för Informationssystem om Arbetsmiljö.

5.2.2. Utbildnings- och informationsinsatser

Förbundets IT-funktion har under 2019 genomfört flera utbildningsinsatser där de flesta väsentliga chefsnivåer och medarbetare inom IT- och informationssäkerhet ingått. Intervjuade uppger att utbildningsinsatserna har nått omkring 100–150 medarbetare, inklusive larmoperatörer.

MSB har en webbaserad utbildning[18] gällande informationssäkerhet som samtliga medarbetare förväntas genomföra. Ansvarig chef ansvarar för att medarbetarna genomför utbildningen. Utbildningen har dock nedprioriterats av flera medarbetare inom organisationen, främst de som arbetar operativt med brand och räddning.

För att nå ut med väsentlig information används intranätet och informationstavlor vid behov, bland annat under intensiva phishingperioder[19] eller för att uppmärksamma användarna på andra typer av incidenter eller hot. Syftet är att ändra användarbeteendet.

5.3. Externt stöd

SSBF har upphandlat en juristfirma som upprätthåller rollen som dataskyddsombud inom förbundet. Ombudets arbete består i regelbundna möten där kommande aktiviteter samt aktuella frågeställningar inom GDPR-området diskuteras. Förbundet har möjlighet att avropa hjälp vid direkta frågor från verksamheten inom sakområden där organisationens egen kontaktperson[20] i GDPR-frågor inte har kompetens.

Förbundet har 2018–2019 anlitat konsulter för att analysera och testa IT-säkerheten inför processkartläggning och informationsklassning. Månatlig uppföljning av säkerhetsläget i IT-miljön genomförs med IT-säkerhetsleverantören.

Förbundet har 2019 upphandlat en ny IT-driftleverantör efter beslut av förbundsdirektör. Detta bland annat med anledning av kvalitetsbrister hos föregående leverantör. Verksamheten har nu en högre leveranskvalitet. För IT-driftleverantören genomförs uppföljning enligt avtalad samverkansmodell avseende leverans, kvalitet, pris och kompetens.

SSBF ställer enligt uppgift krav på säkerhetsavtal och personer i säkerhetsklass för både IT drift och IT säkerhetsleverantören. Förbundet ställer även krav på att inga externa molntjänster används eller utomstående organisationer är inblandade i tekniskt stöd.

6. Återrapportering

Säkerhetskyddschefen såväl som IT-organisationen har föredragit frågor direkt för förbundets ledningsgrupp, vilken består av förbundsdirektören och de fem avdelningscheferna. Säkerhetskyddschefen rapporterar direkt till förbundsdirektören. Förbundsdirektören har enligt uppgift kontinuerlig dialog med direktionens ordförande, vilket vid behov rör frågor om säkerhet.

Vid genomgång av samtliga sammanträdesprotokoll från december 2018 till november 2019 noteras ingen information rörande IT- och informationssäkerhet. I samband med årsbokslut tar direktionen del av uppföljning av internkontrollplanen, vilken innehåller en risk kopplad till GDPR. Enligt intervjuade ser förbundet över formerna för att utveckla ett systematiskt informationssäkerhetsarbete där regelbunden rapportering ingår.

[18] DISA, MSB:s informationssäkerhetsutbildning
[19] En attack-metod där mottagaren manipuleras att delge känslig information eller liknande
[20] Enhetschef på enheten för förbundsövergripande administration/kansli och kommunikation

7. Svar på revisionsfrågor

Revisionsfråga	Svar
Kan ansvarsfördelningen inom förbundet bedömas vara tydlig med avseende på IT- och informationssäkerhet?	Delvis. Riktlinje för skydd och säkerhet tydliggör roller- och ansvar för säkerhet och säkerhetsskydd, vilket inbegriper IT- och informationssäkerhet. Ansvaret för informationssäkerhetsarbetet är dock inte fullt konkretiserat.
I vilken utsträckning kan fastställda styrdokument (policy, riktlinjer etc.) bedömas vara ändamålsenliga och följs efterlevnaden av dessa upp regelbundet av direktionen?	Ett antal väsentliga policys och riktlinjer är under framtagande. Vi bedömer det angeläget att dessa dokument fastslås och förankras i organisationen för att på ett bättre sätt tydliggöra hur IT- och informationssäkerhet ska hanteras inom verksamheten.
I vilken utsträckning är de riskanalyser som upprättas inom förbundet, med avseende på IT- och informationssäkerhet, ändamålsenliga?	I arbetet med att ta fram internkontrollplan för 2019 har riskanalyser genomförts på förbundsnivå. IT- och informationssäkerhetsrisker finns med i internkontrollplanen. Risk- och sårbarhetsanalyser som genomförs utöver internkontrollarbetet vidrör informationsmängder av olika slag. Verksamheten har genomfört en processkartläggning och påbörjat arbetet med en informationsklassning. En fullständig klassning av informationen väntas bli färdigställd under 2020. Sammantaget bedömer vi att de riskanalyser som genomförs, i allt väsentligt är ändamålsenliga sett till omfattning och syfte.
På vilket sätt säkerställs informationssäkerhet samt funktionalitet och säkerhet i de IT-system som förbundet använder i sin verksamhet?	Förbundet har säkerställt funktionalitet och säkerhet i IT-systemen genom bland annat redundant fiber, brandväggslösningar samt digitalt och fysiskt tillträdesskydd. Förbundet har under året upphandlat en ny IT-driftleverantör med högre leveranskrav samt en IT-säkerhetsleverantör. Flera identifierade åtgärder återstår att genomföra. Utmaningarna rör bland annat avtal kopplade till äldre verksamhetssystem. Det finns även ett behov av att tydliggöra rutinerna mellan HR och IT-funktionen för när medarbetare slutar. Detta för att säkerställa aktualitet bland användarkonton, och förhindra åtkomstmöjligheter för obehöriga. Ett digitalt ärendehanteringssystem skulle enligt intervjuade underlätta detta arbete.
I vilken omfattning används stöd från externa konsulter? Är uppföljning och utvärdering av externa tjänster ändamålsenlig i förekommande fall?	Förbundet använder externa konsulter för IT-säkerhet (analys och kontinuerlig rådgivning), dataskyddsombud samt för att hantera IT-driften. Ja. Förbundet har kontinuerliga uppföljningsmöten med samtliga leverantörer. För IT-driftleverantören genomförs uppföljning enligt avtalad samverkansmodell avseende leverans, kvalitet, pris och kompetens.
I vilken utsträckning är återrapporteringen till direktionen avseende IT- och informationssäkerhet ändamålsenlig?	Det saknas en regelbunden rapportering till direktionen rörande verksamhetens IT- och informationssäkerhet, vilket vi bedömer är en brist.

Stockholm den 24 januari 2020

Madeleine Gustafsson
EY

Anja Zetterberg
EY

Bilaga 1: Källförteckning

Intervjuade funktioner:

- Enhetschef IT, fastighet, intern säkerhet, projekt och miljö
- IT strateg, Enhet IT, fastighet, intern säkerhet, projekt och miljö
- Säkerhetsskyddschef, Enhet IT, fastighet, intern säkerhet, projekt och miljö
- Säkerhetschef, Enhet IT, fastighet, intern säkerhet, projekt och miljö
- Arkivarie, Kansliet

Dokument:

- Verksamhetsplan och budget 2019, beslutad av direktionen den 27 november 2018
- Reglemente för direktionen för kommunalförbundet Storstockholms brandförsvar, fastställd av medlemskommunerna, 2018-03-28
- Förbundsordning för kommunalförbundet Storstockholms brandförsvar, fastställd av medlemskommunerna, 2018-03-28
- Policy för skydd och säkerhet, beslutad av direktionen 2016. Uppdaterad 2019-07-19
- Riktlinjer för skydd och säkerhet, framtagen av säkerhetschef, granskad av enhetschef, 2019-11-11
- Internkontrollplan 2019, godkänd av direktionen den 11 juni 2019
- Sammanträdesprotokoll från december 2018 till november 2019