Granskning av informationssäkerhet och dataskydd

Rapport
Räddningstjänsten Dala Mitt

KPMG AB

2022-12-12

Antal sidor 14

Antal bilagor 1

Innehållsförteckning

1 Sammanfattning

KPMG har av Räddningstjänsten Dala Mitts revisorer fått i uppdrag att göra en översiktlig granskning av förbundets arbete med informationssäkerhet och dataskydd. Uppdraget ingår i revisionsplanen för år 2022.

Syftet med granskningen är att bedöma om direktionen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i förbundet.

Utifrån granskningens resultat är vår sammanfattande bedömning att direktionen inte har säkerställt tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i förbundet. Bedömningen baserar vi på att det inom förbundet inte finns framtagna styrande dokument som reglerar hur arbetet ska bedrivas. Inte heller finns någon fastställd organisation med utsedda funktioner med tillräcklig kompetens för att arbeta med informationssäkerhet och dataskydd. I nuläget saknas ett systematiskt arbete med att identifiera och analysera behov och risker för de informationstillgångar som förbundet hanterar, inklusive personuppgifter, för att säkerställa informationssäkerheten. Direktionen har inte tillsett att det finns etablerade incidenthanteringsrutiner för vare sig informationssäkerhetsincidenter eller personuppgiftsincidenter.

Mot bakgrund av vår granskning rekommenderar vi direktionen att:

- Ge förbundsledningen i uppdrag att, utifrån MSB:s rekommendationer (bilaga 1) och metodstöd (avsnitt 2.4), vidta åtgärder i enlighet med dessa så att förbundet etablerar ett systematiskt och riskbaserat informationssäkerhetsarbete.
- Stärka den interna kontrollen avseende direktionens efterlevnad av dataskyddsförordningen så att personuppgiftshanteringen sker i enlighet med förordningens krav.
- Etablera incidenthanteringsrutiner för informationssäkerhet och personuppgifter där ansvar och process för hanteringen tydliggörs.

2 Bakgrund

KPMG har av revisorerna i Räddningstjänst Dala Mitt fått i uppdrag att genomföra en översiktlig granskning av förbundets arbete med informationssäkerhet och dataskydd. Uppdraget ingår i revisionsplanen för år 2022.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Brister i hanteringen kan leda till både ekonomisk skada och förtroendeskada för organisationen.

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet och måste skyddas mot obehörig åtkomst, såväl externt som internt. Det finns ett flertal lagutrymmen som behöver beaktas i hanteringen av information, inte minst dataskyddsförordningen avseende hantering av personuppgifter.

Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att informationstillgångar har ett tillräckligt skydd. För att kunna hantera det på ett ändamålsenligt sätt krävs att det finns ett systematiskt informationssäkerhetsarbete där flera funktioner är involverade och rätt organiserade för uppdraget.

Med anledning av ovanstående drar revisorerna slutsatsen i sin riskanalys, att arbetet med informationssäkerhet och dataskydd behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen är att bedöma om direktionen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i förbundet.

Granskningen ska besvara följande frågor:

- Finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation med tillräcklig kompetens för att arbeta med informationssäkerhet och dataskydd?
- Finns ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerhet inkl. skydd av personuppgifter?

— Finns etablerade rutiner för incidenthantering för informationssäkerhetsincidenter och personuppgiftsincidenter?

Granskningen avgränsas till informationstillgångar upp till sekretessbelagda uppgifter. Information som lyder under säkerhetsskyddslagen ingår inte.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Tillämpbara interna regelverk, policys och beslut
— MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
— Dataskyddsförordningen

2.3 Metod

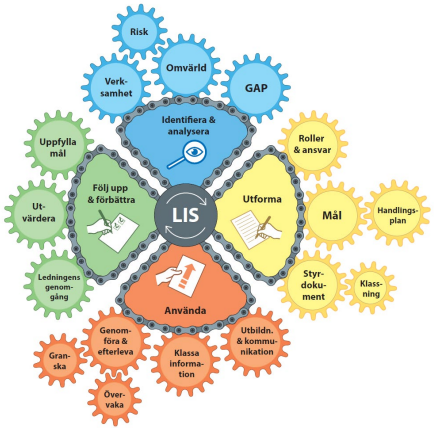
Granskningen har genomförts genom dokumentstudier och intervjuer har genomförts med HR-chef, systemansvarig och verksamhetsstrateg.

Samtliga intervjupersoner har fått möjlighet att faktakontrollera rapporten.

2.4 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet baserat på den internationella standardserien för informationssäkerhet, ISO/IEC 27000, och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

Metodstödet består av fyra olika metodsteg för informationssäkerhetsarbetet vilka illustreras i nedanstående figur.



2.4.1 Identifiera och analyser

Syftet med att analysera informationssäkerhetsarbetet är enligt MSB att säkerställa att informationssäkerheten utformas utifrån verksamhetens rådande förutsättningar. Det ska även leda till att väsentliga informationstillgångar identifieras, vilka risker de ska skyddas mot, samt valda säkerhetsåtgärder.

2.4.2 Utforma

Enligt MSB:s metodstöd behövs följande delar för ett systematiskt informationssäkerhetsarbete:

- Organisation
- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell
- Handlingsplan
- Kontinuitetshantering för informationstillgångar

2.4.3 Använda

När verksamheten har utformat styrningen enligt avsnitt 2.4.2 ska det tillämpas. Det innebär:

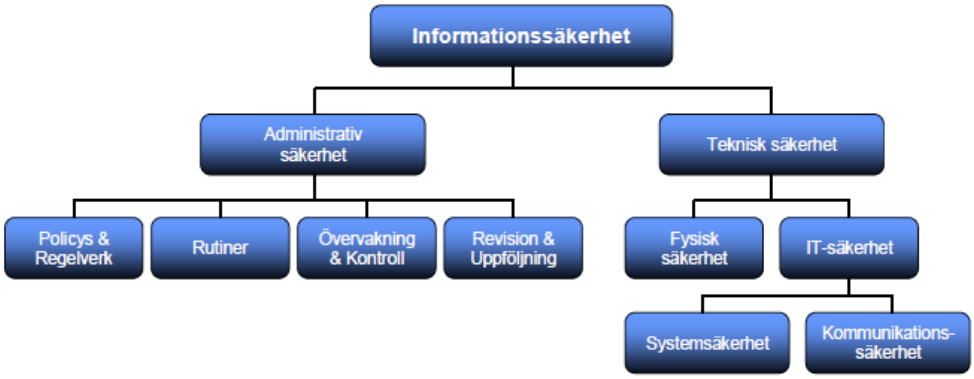
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet.
- Utbilda och kommunicera informationssäkerhetsfrågor till organisationens medarbetare. Det är ständigt pågående arbete som är nödvändigt för att skapa ett systematiskt informationsarbete.

2.4.4 Följa upp och förbättra

Informationssäkerhetsarbetet ska utvärderas och följas upp för att säkerställa att arbetets fortsatta lämplighet, tillräcklighet och verkan. Det kan enligt MSB ske genom övervakning, mätning och måluppföljning.

2.4.5 Roller och ansvar

Informationssäkerhetsbegreppet och dess innehåll kan översiktligt beskrivas i nedanstående skiss:



Informationssäkerhetsarbetet kan struktureras i ett Ledningssystem för informationssäkerhet, kallat LIS. I ett sådant har verksamheten tydliggjort krav som ställs genom styrande dokument och hur ansvaret är fördelat.

En central del i ett ledningssystem, är enligt MSB, ledningens uttalade stöd. Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledningen till chefer och övriga medarbetare. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenhet visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete. En stor del av arbetet med att driva ett ledningssystem handlar därför om att informera medarbetare om de regler som ingår i ledningssystemet.

Den svenska och internationella standardserien SS-ISO/IEC 27000 visar på ett sådant ledningssystem där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad riskanalys, och där informationssäkerhetsarbetet följer en tydlig process. Tillämpning av standarderna enligt denna serie underlättar arbetet med informationssäkerhet inom organisationer och förbättrar också möjligheterna att externt bedöma säkerhet och revidera denna på ett enhetligt sätt.

Enligt MSB:s metodstöd för hur ett systematiskt informationssäkerhetsarbete kan bedrivas framgår det hur ansvaret för arbetet med informationssäkerhet bör fördelas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, verksamhetschefer och medarbetare, tar sitt ansvar för informationssäkerhet i verksamheten.

Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men bör generellt vara placerad nära ledning, exempelvis i ledningsstaben. Vanliga organisatoriska placeringar, enligt MSB:s metodstöd är exempelvis:

- Säkerhet
- Kvalitet
- Juridik

I de fall rollen är placerad i en strategisk IT-funktion bör funktionen vara åtskilda från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetssamordnaren både ska granska och vara kravställande gentemot IT-drift och riskerar annars att brista i opartiskhet.

3 Resultat av granskningen

3.1 Det systematiska informationssäkerhetsarbetet

Styrande dokument

Vi har för granskningen erhållit styrande dokument, bland annat IT-policy, integritetspolicy och information till anställda om hur personuppgifter behandlas utifrån GDPR. Däremot saknar förbundet styrande dokument med koppling till det systematiska informationssäkerhetsarbetet. Inte heller finns några riktlinjer hur personuppgifter ska hanteras eller förtecknas.

Vid intervjuer framkommer att det pågår ett arbete att ta fram riktlinjer och arbetssätt utifrån säkerhetsskyddslagen och säkerhetsskyddsförordningen, där informationssäkerhet med fokus sekretessbelagda uppgifter som har betydelse för totalförsvarets eller Sveriges säkerhet ingår. Detta arbete ingår däremot inte i avgränsningen för denna granskning.

Organisation och kompetens

Det finns ingen utsedd funktion för informationssäkerhet inom förbundet. Enligt intervjuade finns en utsedd systemägare för varje system inom förbundet. Dock varierar kunskapen om uppdraget mellan systemägarna. Förbundet har utsett ett dataskyddsombud, vilket är en tjänsteperson i Falu kommun.

HR-chefen har haft i uppdrag att ta fram anvisningar för hur förbundet hanterar medarbetares personuppgifter och en integritetspolicy som beskriver hur medborgares personuppgifter hanteras. Samtliga medarbetare har fått information om anvisningarna och integritetspolicyn ska publiceras på förbundets hemsida.

Samtliga medarbetare i förbundet har genomfört en tvådelad interaktiv utbildning avseende hantering av personuppgifter och informationssäkerhet. Den sista delen av utbildningen genomfördes i augusti i år. Utöver det har HR-chefen genomfört två utbildningar för förbundets ledningsgrupp rörande GDPR och personuppgiftshantering.

Analys av behov och risker för informationssäkerhet

Eftersom skadeverkningarna av bristande säkerhet i system även medför risker hos andra informationsägare och verksamheter behöver riskbedömning och kravställningar om åtgärder ske med samsyn och med delaktighet från olika funktioner i förbundet.

Av intervjuer framgår att det varken finns riktlinjer eller etablerade arbetssätt för att klassa informationen i förbundets system. Ingen tjänsteman har ansvar att genomföra riskbedömning och informationsklassning av verksamhetssystem och ingen informationsklassning har genomförts.

Av intervjuade framkommer att det pågår ett arbete att upprätta registerförteckningar för de personuppgiftsbehandlingar som förbundet i nuläget har. Arbetet är fördelat i ledningsgruppen, baserat på tjänstemännens ansvarsområden. Förbundets dataskyddsombud används som stöd i arbetet. För personuppgiftsbehandlingar där känsliga personuppgifter hanteras har förbundet genomfört konsekvensbedömningar, vilket är ett krav i enlighet med dataskyddsförordningen.

Incidenthantering

Vid granskningen framkommer att det finns en rutin avseende incidenthantering IT från 2022-09-07 som beskriver IT-enhetens interna hantering vid incidenter. Däremot saknas det inom förbundet en rutin för hur medarbetare ska agera vid personuppgiftsincidenter och informationssäkerhetsincidenter. Vid en personuppgiftsincident som inträffade nyligen, hanterades incidenten efter bästa förmåga i dialog med förbundets utsedda dataskyddsombud.

4 Slutsats och rekommendationer

Utifrån granskningens resultat är vår sammanfattande bedömning att direktionen inte har säkerställt tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i förbundet.

Bedömningen baserar vi på att det inom förbundet inte finns framtagna styrande dokument som reglerar hur arbetet ska bedrivas. Inte heller finns någon fastställd organisation med utsedda funktioner med tillräcklig kompetens för att arbeta med informationssäkerhet och dataskydd. I nuläget saknas ett systematiskt arbete med att identifiera och analysera behov och risker för de informationstillgångar som förbundet hanterar, inklusive personuppgifter, för att säkerställa informationssäkerheten. Direktionen har inte tillsett att det finns etablerade incidenthanteringsrutiner för vare sig informationssäkerhetsincidenter eller personuppgiftsincidenter.

Utifrån vår bedömning och slutsats rekommenderar vi direktionen att:

- Ge förbundsledningen i uppdrag att, utifrån MSB:s rekommendationer (bilaga 1) och metodstöd (avsnitt 2.4), vidta åtgärder i enlighet med dessa så att förbundet etablerar ett systematiskt och riskbaserat informationssäkerhetsarbete.
- Stärka den interna kontrollen avseende direktionens efterlevnad av dataskyddsförordningen så att personuppgiftshanteringen sker i enlighet med förordningens krav.
- Etablera incidenthanteringsrutiner för informationssäkerhet och personuppgifter där ansvar och process för hanteringen tydliggörs.

Räddningstjänsten Dala Mitt
Granskning av informationssäkerhet och dataskydd

2022-12-12

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Linnéa Grönvold
Certifierad kommunal revisor

Bilaga 1 MSB:s rekommendationer[1]

1. ***Utse en funktion för informationssäkerhet***
   Funktionens placering bör vara direkt underställd högsta ledningen och funktionen bör använda en majoritet av sin tid till informationssäkerhetsuppdraget.

2. ***Ta fram analys av nuläget***
   Gör en verksamhetsanalys för att få kunskap om organisationens processer, vilken information som hanteras samt vilket behov av skydd som finns.

3. ***Informera ledningen hur nuläget ser ut***
   Visa exempel på reella hot och inträffade incidenter.

4. ***Skapa en handlingsplan utifrån nuläget***
   Ta fram styrdokument, policy och riktlinjer och åtgärda de viktigaste bristerna och sårbarheterna.

5. ***Klassa informationen***
   Klassa informationen efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet.

6. ***Höj säkerhetsmedvetandet***
   Ge stöd till organisationens förmåga att efterleva kraven i framtagna riktlinjer.

7. ***Ta fram informationssäkerhetsrelaterade krav som används vid upphandlingar***
   Se till att identifiera informationssäkerhetskraven och etablera en process för att få med kraven i upphandlingar.

8. ***Gör uppföljningar***
   Se över om förbundet efterlever det som står i de framtagna riktlinjerna. Planera in återkommande uppföljning av verksamheten.

[1] rekommendationer_kommuner_170113_kb.pdf (informationssakerhet.se)