Granskning av informationssäkerhet

Rapport
Askersundsbostäder AB

KPMG AB

2023-01-25

Antal sidor 19

Askersundsbostäder AB
Granskning av informationssäkerhet

2023-01-25

Innehållsförteckning

1 Sammanfattning

KPMG har av lekmannarevisorn i Askersundsbostäder AB fått i uppdrag att genomföra en granskning av bolagsstyrelsens informationssäkerhetsarbete.

Utifrån genomförd granskning är vår sammanfattande bedömning att styrelsen till viss del har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten inom bolaget.

Vår bedömning är att bolagsstyrelsen och VD behöver ta ett större ansvar för informationssäkerheten för att organisationen ska bedömas ändamålsenlig. Vi uppfattar att IT-ansvarig, som är extern konsult, har ett alltför stort ansvar i arbetet i relation till övriga linjechefer i verksamheten samt i förhållande till mandat och befogenheter. Vi vill dock poängtera att vi inte funnit några brister i utövandet och att det arbete som genomförts av funktionen har lagt en god grund för bolagets informations-säkerhetsarbete.

Det finns upprättade styrande dokument som i vissa delar tydliggör ansvar, kravställning och hur informationssäkerhetsarbetet ska bedrivas på övergripande nivå. Det saknas uppgift på att nuvarande dokument har beslutats av styrelsen så att de är formellt antagna. Informationssäkerhetspolicyn eller kompletterande riktlinjer bör även revideras med beskrivning av bolagsstyrelsens ansvar för informationssäkerhetsfrågorna.

I nuläget sker en viss kravställning på tekniska åtgärder utifrån riskbedömningar och klassningar. Dock saknar arbetet med riskanalys och klassning systematik och är därtill personberoende. Vi uppfattar att IT-säkerhetsåtgärder som IT-ansvarig bedömer att det finns behov av implementeras för de informationstillgångar som hanteras i bolagets system. Vår bedömning är att det finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.) där utveckling och införande av nya verktyg sker löpande för att säkerheten ska möta nya hot och risker. De implementerade säkerhetsåtgärderna har till viss del följts upp genom att regelbundet övervaka säkerhetshändelser och analysera dess konsekvenser för att kunna förbättra informationssäkerheten avseende den tekniska säkerheten.

I nuläget saknas i övrigt uppföljning av det informationssäkerhetsarbete som genomförs inom bolaget för övriga aspekter av informationssäkerheten i form av administrativ och organisatorisk säkerhet. Det finns incidenthanteringsrutiner men vi ser behov av att stärka kännedom om vad som är incidenter och hur dessa, om de sker, ska hanteras.

Utifrån vår bedömning och vår slutsats rekommenderar vi styrelsen för Askersundsbostäder att:

- Avseende styrande dokument för informationssäkerhet:
  - Revidera policy med beskrivning av bolagsstyrelsens ansvar.
  - Revidera policy med beskrivning av hur uppföljning av informationssäkerhetsarbetet ska genomföras.
  - Bedöma om det finns behov av kompletterande anvisningar för hur informationssäkerhetsarbetet ska genomföras inom bolaget, exempelvis utifrån MSB:s metodstöd, vilket presenteras i avsnitt 2.4.
  - Fatta beslut om de styrande dokument som ska utgöra styrning för bolagets informationssäkerhetsarbete och förankra dessa i verksamheten.
- Tillse att verksamhetsansvariga upprätthåller sitt linjeansvar för informationssäkerhet genom att ta ansvar och delta i aktiviteter i arbetet, främst avseende riskanalyser och informationsklassning.
- Etablera en regelbunden uppföljning av informationssäkerhetsarbetet, där efterlevnad av styrdokument ingår som en del.

2 Bakgrund

KPMG har av lekmannarevisorerna i Askersundsbostäder AB fått i uppdrag att genomföra en granskning av bolagsstyrelsens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om informationssäkerhet för information som hanteras i kommuners och dess bolags IT-system. Alltmer information hanteras idag med olika tekniska lösningar och aldrig förr har kommuner och bolag hanterat sådana mängder information som görs idag. Informationssäkerhet innebär att skydda information utifrån dess krav på konfidentialitet, riktighet och tillgänglighet i alla kommunens system. För att kunna hantera detta på ett ändamålsenligt sätt krävs att kommuner och bolag har ett systematiskt informationssäkerhetsarbete där flera funktioner är involverade och rätt organiserade för uppdraget. Informationssäkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av bolagets kärnverksamheter.

Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod. Många verksamheter inom kommuner och bolag är idag helt beroende av väl fungerande IT. För flera verksamheter handlar ett väl fungerande IT-stöd såväl om säkerhet som möjlighet till en fungerande verksamhet utan driftstörningar. Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd.

Med anledning av ovanstående drar lekmannarevisorerna slutsatsen i sin riskanalys, att informationssäkerhetsarbetet behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningens syfte har varit att bedöma om styrelsen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i bolaget.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhet?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?
- Sker en kravställning av IT-säkerhetsåtgärder utifrån genomförd riskbedömning och klassning av informationstillgångar som hanteras i system?
- Finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.)?
- Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?
- Görs systematiska uppföljningar av implementerade säkerhetsåtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

Granskningen omfattar bolagsstyrelsen för Askersundsbostäder AB och avser år 2022.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

- Kommunallagen 6 kap. 9 §
- Aktiebolagslagen
- Bolagsordning
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- Interna styrdokument

2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstemän.

I granskningen har följande funktioner intervjuats:

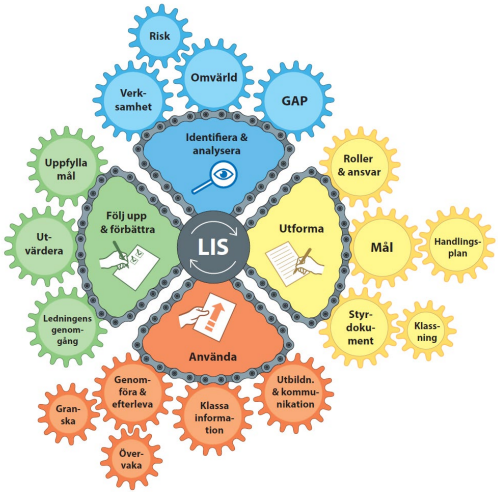
- Administratör
- IT-ansvarig (extern konsult)

De intervjuade 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 Identifiering och analys

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 Utformning

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

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

2.4.3 Användning

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

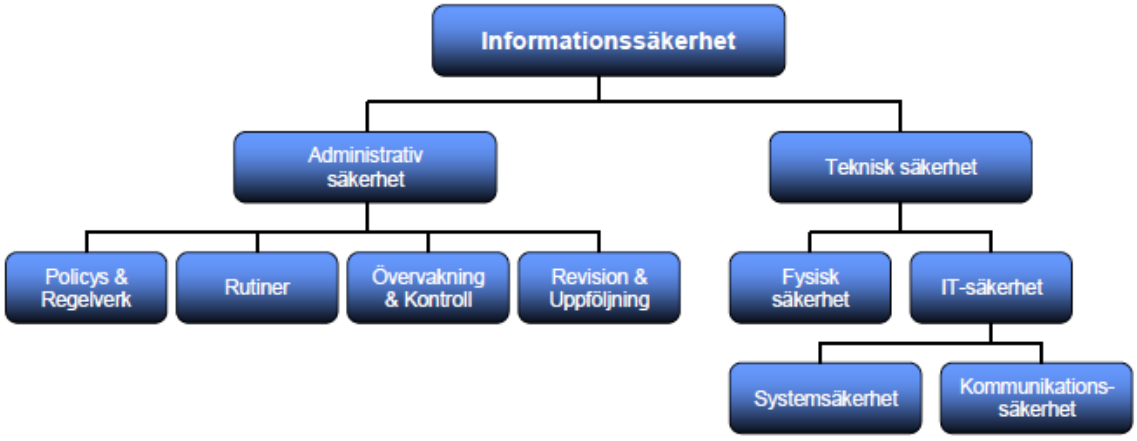
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet.
- Utbilda och kommunicera informationssäkerhetsfrågor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

2.4.4 Uppföljning och förbättring

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 Organisation och ansvar

3.1.1 Styrande dokument

Bolagets informationssäkerhetsarbete utgår från en beslutad informationssäkerhetspolicy.[1] Policyn syftar till att säkerställa att all information inom bolaget hanteras säkert och effektivt. Policyn beskriver principerna om tillgänglighet, riktighet, konfidentialitet och spårbarhet.

I policyn anges att informationssäkerhetsarbetet ska ske utifrån etablerade standarder och internationella riktlinjer och i övrigt utföras enligt bolagets rutiner. Policyn beskriver generella riktlinjer för bolagets informationssäkerhetsarbete. Bland annat framgår information om informationsklassning och riskbedömning, åtkomst och behörighet, loggning och uppföljning samt incidenthantering och outsourcing.

Informationssäkerhetsarbetet är indelat mellan fysisk säkerhet, personuppgifter och IT-säkerhet. I policyn framgår att det ska finnas kompletterande styrdokument inom respektive område.

Vi har tagit del av beslutad IT-policy[2] som bland annat innehåller riktlinjer för hantering av information och utrustning, användning av internet och e-post, lösenordshantering och ansvar. Revidering av policyn pågår men ny version hade inte fastställts vid tiden för granskningen.

Vidare framgår ett antal informationspunkter rörande IT-säkerhet av dokumentet. Här anges bland annat att:

- Bolagets nätverk ska vara skyddat mot intrång.
- Riskanalyser tas fram innan större förändringar genomförs.
- Information ska skyddas genom backup-system.
- Varje dator ska ha ett antivirusprogram installerat där uppdateringar sker automatiskt.
- Bolagets IT-ansvarige ansvarar för underhåll och drift och ska regelbundet kontrollera IT-säkerheten.

[1] Policyn är framtagen av bolagets IT-avdelning och senast reviderad 2022-10-11.

[2] Beslutad 2018-02-20. Beslutsinstans framgår ej.

3.1.2 Roller och ansvar

Informationssäkerhetspolicyn beskriver roll- och ansvarsfördelningen inom informationssäkerhetsarbetet på en övergripande nivå.

Det anges att policyn gäller för bolagets anställda och konsulter, samt övriga kontraktsbundna intressenter. I informationssäkerhetspolicyn anges följande ansvarsfördelning för de tre säkerhetsområdena som informationssäkerheten är indelad i:

- VD ansvarar för den övergripande säkerhetsadministrationen och policydokument samt utbildningsfrågor.
- Bolagets fastighetsförvaltare ansvarar för den fysiska säkerheten
- IT-ansvarig ansvarar för IT-säkerheten
- Integritetsansvarig ansvarar över dataskydd och personuppgiftshantering. Av policyn framgår att denna roll innehas av VD.

Bolagets IT-ansvarig anlitas genom avtal. Den externa konsulten har arbetat med bolagets IT-frågor sedan 2007. I intervju beskrivs att uppgifterna för konsulten omfattar det tekniska arbetet med it-infrastruktur som datorer, servrar, nätverk mm. IT-ansvarig är även involverad i verksamhetsfrågor inom IT-området. IT-ansvarig upprättar exempelvis styrdokument, regler, riskanalyser mm. Vi uppfattar i intervju att IT-ansvarig även genomför kontroller och granskningar inom bolaget, exempelvis avseende GDPR för att säkerställa att bolaget lever upp till de krav som finns.

Vi uppfattar av intervjuer att det främst är IT-ansvarig som genomför det strategiska och operativa arbetet inom både informations- och IT-säkerhet inom bolaget. Intervjuade uppger att verksamheten fungerat väl trots längre frånvaro av IT-ansvarig vilket enligt intervjuade har påvisat att bolaget kan hantera vissa frågor internt utan stöd från konsulten.

För personuppgiftshantering finns ett mer delegerat arbete där ansvariga inom olika avdelningar har i ansvar att upprätta registerförteckningar för de personuppgiftsbehandlingar som hanteras.

I styrande dokument anges inget ansvar för bolagsstyrelsen. Intervjuade anger att det skulle vara önskvärt med ett större engagemang och insyn i informations-säkerhetsarbetet från styrelsens sida. I nuläget saknas etablerad rapportering till bolagsstyrelsen om informationssäkerhetsarbetet eller tillhörande risker.

3.1.3 Bedömning

Vår bedömning är att det till viss del finns upprättade styrdokument som tydliggör ansvar, vilka krav som ställs och hur informationssäkerhetsarbetet ska bedrivas. Nuvarande informationssäkerhetspolicy saknar uppgift om vem som beslutat om den och vi uppfattar att övriga styrande dokument inte har fastställts av bolagsstyrelsen.

I informationssäkerhetspolicyn saknas ansvarsbeskrivning för bolagsstyrelsen vilket vi anser är en brist. Detta då styrelsen är övergripande ansvariga för bolagets säkerhetsarbete, dels är personuppgiftsansvariga utifrån dataskyddsförordningens krav. I det ansvaret behöver de säkerställa att bolagets informationssäkerhetsarbete bedrivs med en systematik för att skydda informationstillgångarna. Det har inte genomförts någon uppföljning av att de styrande dokumenten efterlevs inom bolaget.

Vår bedömning är att bolagsstyrelsen och VD behöver ta ett större ansvar för informationssäkerheten i bolaget för att organisationen ska vara ändamålsenlig. Vi uppfattar att IT-ansvarig, som är extern konsult, har ett alltför stort ansvar i arbetet i relation till övriga linjechefer i verksamheten samt i förhållande till mandat och befogenheter. Funktionen upprättar och fastställer i nuläget de styrdokument som gäller inom området och är även den som operativt verkställer arbetet i enlighet med styrande dokument. Vi vill dock understryka att vi inte ser några brister med det arbete som genomförts av IT-ansvarig vilket i stora delar har medfört att bolaget har ett pågående informationssäkerhetsarbete.

3.2 Riskanalys och säkerhetsåtgärder

I informationssäkerhetspolicyn regleras att känslig och väsentlig information som hanteras inom bolaget ska klassificeras för att avgöra vilket skydd som behövs. Tillsammans med klassificeringen ska riskbedömningar avgöra vilka säkerhetsåtgärder som behövs för respektive informationstyp. Riskbedömningar ska genomföras löpande samt alltid vid större förändringar.

Enligt uppgift genomför bolaget riskanalyser avseende informationssäkerhet i viss utsträckning. Riskanalyserna genomförs i sådana fall av IT-ansvarig. Informationsklassningar har inte genomförts i enlighet med beslut i policyn.

Utifrån resultatet av riskanalyser föreslår IT-ansvarig tekniska åtgärder som godkänns av VD innan de implementeras.

Exempel på åtgärder är redundans för nätverk och servrar, stärkt säkerhet vid inloggning genom införande av tvåfaktorsautentisering och kartläggning av information som hanteras i molnbaserade system. Intervjuade beskriver att IT-ansvarig löpande analyserar säkerhetsloggar för att identifiera hot och vidta åtgärder för de system och plattformar som nyttjas inom bolaget. En policy finns fastställd för bolaget arbete med säkerhetskopiering. Intervjuade uppger att rutinerna följer det som regleras av policyn och att återläsning av data testas regelbundet för att säkerställa att ingen information förloras eller skadas.

I nuläget saknas dokumenterade kontinuitetsplaner och intervjuade uppger att det är ett utvecklingsområde att dokumentera rutiner och processer för det IT- arbete som genomförs inom bolaget.

3.2.1 Bedömning

Vår bedömning är att riskanalyser till viss del upprättats i enlighet med styrande dokument men att det i nuläget inte sker tillräckligt systematiskt. Vi anser därtill att riskanalyser och informationsklassning ska göras efter initiativ från VD samt linjeansvariga chefer i samråd med IT-ansvarig och inte som i nuläget då IT-ansvarig genomför detta arbete på egen hand. Den information som hanteras inom bolaget har därigenom inte klassificerats utifrån informationstyper för att bedöma dess skyddsvärde så att det kan utgöra underlag för införande av relevanta skyddsåtgärder. Vår bedömning är dock att IT-säkerhetsåtgärder som IT-ansvarig bedömer att det finns behov av implementeras för de informationstillgångar som hanteras i bolagets system.

Vår bedömning är att det finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.) där utveckling och införande av nya verktyg sker löpande för att säkerheten ska möta nya hot och risker.

De implementerade säkerhetsåtgärderna har till viss del följts upp genom att regelbundet övervaka säkerhetshändelser och analysera dess konsekvenser för att kunna förbättra informationssäkerheten avseende den tekniska säkerheten.

I nuläget saknas i övrigt uppföljning av det informationssäkerhetsarbete som genomförs inom bolaget för övriga aspekter av informationssäkerheten i form av administrativ och organisatorisk säkerhet.

3.3 Incidenthantering

I bolagets informationssäkerhetspolicy finns beskrivet hur hantering ska ske vid säkerhetsincidenter. Av beskrivningar framgår att den som upptäcker brister i informationssäkerheten måste uppmärksamma chef eller säkerhetsfunktionen. Alla medarbetare måste också rapportera händelser som kan göra att informationstillgångar utsätts för risker. Incidenter ska dokumenteras genom incidentrapport som upprättas hos ansvarig avdelning.

I bolaget finns även etablerade rutiner för personuppgiftsincidenter.[3] Av rutinen framgår tillvägagångsätt för medarbetare vid misstanke om en personuppgiftsincident. Här framgår att medarbetare omgående ska rapportera misstanke om sådana incidenter till dataskyddsansvarig eller närmsta chef.

Av rutinen framgår även hanteringen efter incidenten anmälts. Bland annat anges att risker utifrån incidenten ska bedömas och att incidenter ska dokumenteras. Rutinen beskriver även hur åtgärder ska vidtas för att förhindra framtida incidenter, tillvägagångssätt för anmälan till Integritetsskyddsmyndigheten samt hur uppföljning ska genomföras.

Intervjupersoner uppger att en utbildning har genomförts under 2022 inom både GDPR och inom informationssäkerhet. I utbildningen ingick bland annat IT-säkerhet och risker i IT-användning, exempelvis bluffmejl. Uppföljning av utbildningar har inte genomförts.

Intervjuade beskriver vidare att det inte anmälts några incidenter under året så det har inte funnits behov av rapportering. Även om utbildning genomförts så framgår av intervjuer att det finns risk för mörkertal för incidenter, att sådana sker utan att personal ser det som allvarligt nog för att det ska anmälas.

[3] Beslutsdatum eller instans framgår inte av dokumentet.

3.3.1 Bedömning

Vår bedömning är att det finns dokumenterade incidenthanteringsrutiner för informationssäkerhets- och personuppgiftsincidenter. Vi bedömer dock att det kan finnas en viss risk att dessa incidenter inte upptäcks och rapporteras i tillräckligt hög grad.

Vår bedömning är att det finns förmåga att upptäcka it-incidenter genom den analys av säkerhetsloggar som genomförs regelbundet. Därtill finns en god överblick av it-miljön av IT-ansvarig. Vi vill dock påtala att nuvarande bemanning är personberoende och ansvarsfördelningen kan utgöra en sårbarhet vid en allvarlig säkerhetshändelse där ett skyndsamt agerande kan krävas för att minska skadeverkan av ett eventuellt intrång eller annan allvarlig störning.

4 Slutsats och rekommendationer

Utifrån genomförd granskning är vår sammanfattande bedömning att styrelsen till viss del har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten inom bolaget.

Vår bedömning är att bolagsstyrelsen och VD behöver ta ett större ansvar för informationssäkerheten för att organisationen ska bedömas ändamålsenlig. Vi uppfattar att IT-ansvarig, som är extern konsult, har ett alltför stort ansvar i arbetet i relation till övriga linjechefer i verksamheten samt i förhållande till mandat och befogenheter. Vi vill dock poängtera att vi inte funnit några brister i utövandet och det arbete som genomförts av funktionen har lagt en god grund för bolagets informationssäkerhetsarbete.

Det finns upprättade styrande dokument som i vissa delar tydliggör ansvar, kravställning och hur informationssäkerhetsarbetet ska bedrivas i stort. I nuläget sker en viss kravställning på tekniska åtgärder utifrån riskbedömningar och klassningar. Dock så saknar arbetet med riskanalys och klassning systematik och är därtill personberoende. Vi uppfattar att IT-säkerhetsåtgärder som IT-ansvarig bedömer att det finns behov av implementeras för de informationstillgångar som hanteras i bolagets system.

I nuläget saknas uppföljning av det informationssäkerhetsarbete som genomförs och efterlevnad av styrande dokument har inte kontrollerats

4.1 Rekommendationer

Utifrån vår bedömning och vår slutsats rekommenderar vi bolagsstyrelsen att:

- Avseende styrande dokument för informationssäkerhet:
  - Revidera policy med beskrivning av bolagsstyrelsens ansvar.
  - Revidera policy med beskrivning av hur uppföljning av informationssäkerhetsarbetet ska genomföras.
  - Bedöma om det finns behov av kompletterande anvisningar för hur informationssäkerhetsarbetet ska genomföras inom bolaget, exempelvis utifrån MSB:s metodstöd, vilket presenteras i avsnitt 2.4.
  - Fatta beslut om de styrande dokument som ska utgöra styrning för bolagets informationssäkerhetsarbete och förankra dessa i verksamheten.

- Tillse att verksamhetsansvariga upprätthåller sitt linjeansvar för informationssäkerhet genom att ta ansvar och delta i aktiviteter i arbetet, främst avseende riskanalyser och informationsklassning.
- Etablera en regelbunden uppföljning av informationssäkerhetsarbetet, där efterlevnad av styrdokument ingår som en del.

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Linnéa Grönvold
Certifierad kommunal revisor