Osby kommun

Granskning IT- och informationssäkerhet
Juni 2022

Building a better working world

Sammanfattning

På uppdrag av Osby kommuns förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Följande revisionskriterier användes:

- Myndigheten för samhällsskydd och beredskaps (MSBs) styrmodell för offentliga organisationers IT- och informationssäkerhet, LIS.
- ISO/IEC 27000 standarden för informationssäkerhet.
- God praxis och EY:s erfarenhet inom IT-, cyber - och informationssäkerhet.

Granskningen genomfördes från mars till juni 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation. Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, "Granskningsprogram Cyber- och Informationssäkerhet" (GCI), särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 57 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive områdena. Representanter för kommunens informationssäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Osby kommun ha en genomsnittlig mognadsgrad på 1,78 vilket är en markant lägre mognadsgrad än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,49. Detta är en betydligt lägre mognadsgrad än vad EY rekommenderar för en kommun likt Osby, givet den mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras. Granskningsresultatet indikerar att kommunens mognadsgrad är något högre avseende personuppgifter och lägst inom drift och programförändringar.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Osby kommun tillser att:

- En kontinuitetsplan upprättas, beslutas och implementeras.
- Styrdokument upprättas och implementeras inom ett flertal identifierade områden avseende kommunens IT- och informationssäkerhetsarbete.
- En utbildningsplan upprättas avseende IT- och informationssäkerhet.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Building a better working world

Innehållsförteckning

1 Bakgrund

Osby kommun hanterar stora mängder digital information inom alla dess verksamheter. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig samt har tillräckligt starkt skydd.

Kommunrevisorerna har valt att genomföra en granskning för att kartlägga kommunens arbete med IT- och informationssäkerhet. Riskerna inom dessa områden är inte enbart relaterade till Osby kommun utan gäller hela den offentliga sektorn.

1.1 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i kommunens interna kontroll kopplat till säkerställande av att arbetet med IT- och informationssäkerhet är ändamålsenligt. Vidare är syftet också att bedöma i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande övergripande revisionsfråga:

- Bedriver Osby kommun ett tillräckligt och ändamålsenligt IT- och informationssäkerhetsarbete?

Revisionsfrågan bryts ned och besvaras genom följande underliggande revisionsfrågor:

- Kan *styrningen* av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?
- Är arbetet med att *följa upp* att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?
- Är Osby kommuns *incidenthanteringsprocess* ändamålsenlig?

1.2 Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policyer. Granskningen är begränsad till arbetet som Osby kommun bedriver på central nivå. Intervjuer har endast utförts med representanter på central nivå och inte med representanter från nämnder eller förvaltningen. Inga bolag har granskats. Ingen teknisk analys har genomförts och inga stickprov på efterlevnad har tagits.

1.3 Metod och genomförande

Granskningen har byggt på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor. Ramverket omfattar flera områden vilka

täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i IT- och informationssäkerhet.

Inledningsvis har relevant dokumentation kring kommunens rutiner och processer granskats av EY. Därefter har granskningsmöten hållits med kommunens representanter för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av IT- och informationssäkerhet i kommuner. Under granskningen har dock inga stickprovstester utförts, vilket innebär att själva efterlevnaden av kommunens rutiner och kontroller inte testas. Slutligen har den samlade bilden av dokumentation samt information inhämtad via granskningsmöten analyserats och bedömts.

Under granskningen har följande roller intervjuats:

- Administrativ chef
- Säkerhetschef/säkerhetsskyddschef
- Dataskyddssamordnare
- Konsult från kommunens samägda IT-bolag

De intervjuade personerna har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

Fullständig källförteckning framgår av bilaga 1.

Under uppdraget har EY granskat 5 huvudområden som brutits ner på 18 underområden enligt nedan.

Styrning

- Ledningssystem
- Policy
- Strategi och rutiner
- Organisation

Personal och behörigheter

- Personal
- Behörighetshantering

Drift

- Incidenthantering
- Informationsklassning
- Nätverk
- Brandväggar
- Kontinuitetsplanering

Programförändringar

- Förändringshantering

Personuppgifter

- Personuppgiftsstyrning
- Personuppgiftsbehandling
- Personuppgiftsrutiner
- Dataskydd
- Utbildning inom dataskyddsförordningen
- Molntjänster

Under granskningen har EY gjort en sammanfattande betygsättning på samtliga 18 underområden på en skala 1-5. Skalans definition presenteras nedan:

Tabell 1: Skala för bedömning av Osby kommuns mognadsgrad inom informationssäkerhetsområden

1	Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc
2	Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning
3	Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen
4	Förutom väldokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning
5	Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan till exempel ett område med grön färgkod ändå sakna viktiga delar. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

Tidsplanen för arbetet såg ut enligt följande:

Tabell 2: Tidsplan för IT- och informationssäkerhetsgranskningen

Förberedelser och planering	Mars 2022
Insamling och analys av dokumentation	April 2022
Arbetsmöte	April 2022
Rapportskrivning samt intern kvalitetssäkring	April 2022
Faktagranskning av kommunen	Maj 2022
Justering samt färdigställande av rapport	Maj 2022
Avrapportering och slutpresentation	Juni 2022

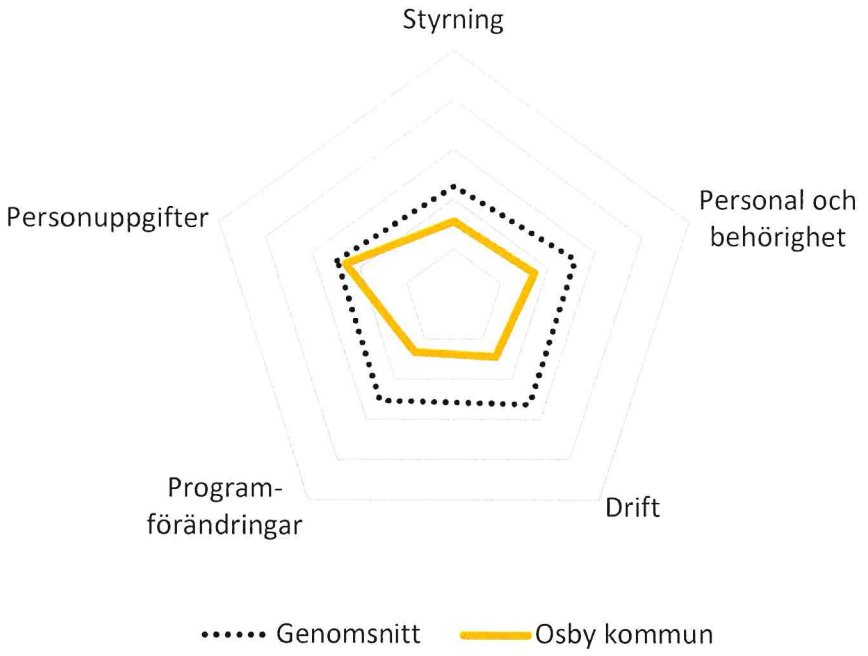
2 Analys

Baserat på den analys och granskning som genomförts bedöms Osby kommun ha en genomsnittlig mognadsgrad på 1,78 av 5,0 vilket är en markant lägre mognadsgrad än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,49. Mognadsgraden för Osby kommun är betydligt lägre än vad EY rekommenderar för en kommun, givet den mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras. Granskningsresultatet indikerar att kommunens mognadsgrad är något högre avseende personuppgifter och lägre inom drift och programförändringar.

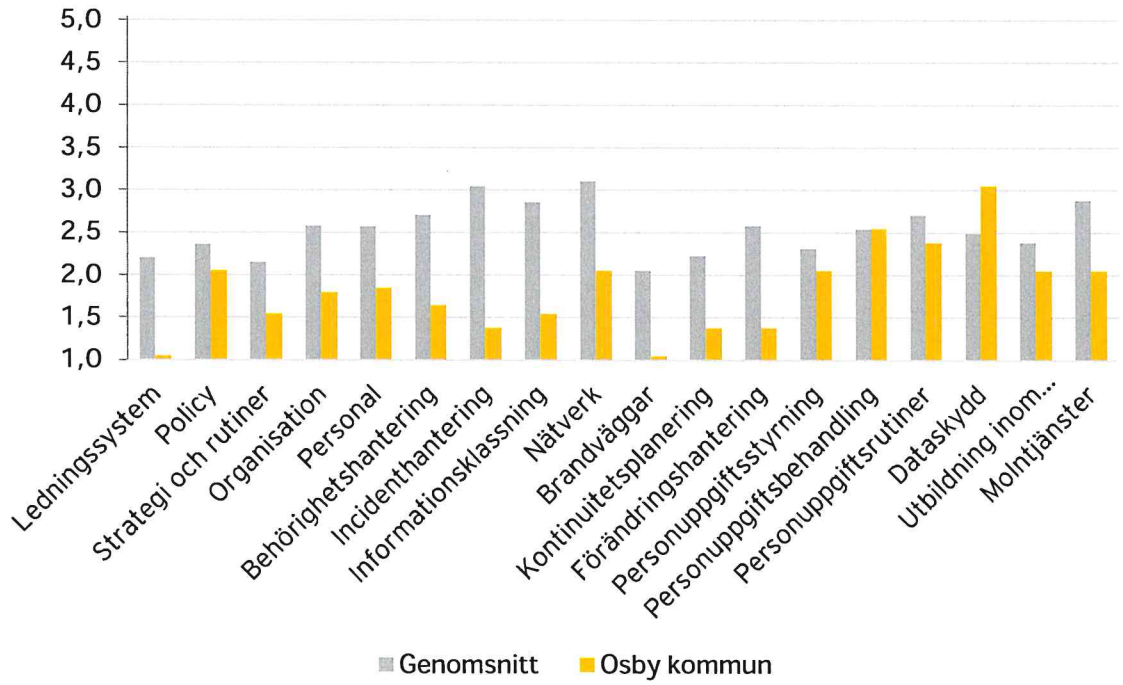
Osby kommun arbetar för att utveckla informationssäkerhetsarbetet. Bland annat bedrivs ett arbete för att anställa inom säkerhetsområdet, där fokus på rekryteringen dock inte ligger på informationssäkerhet specifikt. Därtill ses samtliga styrdokument över för att säkerställa att kommunen endast behåller styrdokument som anses vara nödvändiga för att bedriva arbetet med informationssäkerhet på ett effektivt och ändamålsenligt sätt. Vidare bedrivs ett arbete för att implementera kontroll av efterlevnad av policy och riktlinjer inom informationssäkerhetsområdet.

Kommunens främsta behov till förbättring ligger i upprättandet av styrdokument inom informationssäkerhetsområdet samt säkerställa att dessa förblir riktiga och aktuella över tid. Vidare finns det behov av en utbildningsplan med obligatoriska utbildningstillfällen med möjlighet till uppföljning. Det finns även förbättringspotential gällande löpande efterlevnadskontroll med rapportering till kommunstyrelsen.

Figur 1 nedan redovisar kommunens mognadsgrad för de 5 huvudområden som granskats samt en jämförelse med andra kommuner av motsvarande storlek och karaktär. Figur 2 visar detsamma fast nedbrutet på 18 underområden. Genomsnittet för andra kommuner av motsvarande storlek och karaktär är framtaget genom att bedöma mognadsgrad för samma områden och enligt samma metod som för Osby kommun.



Figur 1: Överblick över kommunens mognadsgrad för de 5 huvudområden som granskats i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.



Figur 2: Överblick över kommunens mognadsgrad för de 18 underområden i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.

2.1 Styrning

I sektionen nedan beskrivs nulägesbilden för huvudområdet *styrning* samt de iakttagelser som noterats under granskningens utförande (se Tabell 3).

Tabell 3: Nuläge och iakttagelser inom huvudområdet Styrning

Område	Nuläge	Iakttagelser	Mognad
Ledningssystem	Kommunen har inte implementerat något ledningssystem för informationssäkerhet. Framöver ska möjligheten att införa ett ledningssystem för informationssäkerhet ses över, med vid tid för granskning finns det inte någon utarbetad plan för när detta kommer ske.	Inget ledningssystem för informationssäkerhet är implementerat.	1,00
Policy	Kommunen har en övergripande säkerhetspolicy som innefattar områdena informationssäkerhet, brottsförebyggande, säkerhet, säkerhetsskydd, krisberedskap och civilt försvar. Säkerhetspolicyn beslutades av kommunfullmäktige under 2021 och gäller för samtliga nämnder, förvaltningar och kommunala bolag inom Osby kommun. Säkerhetspolicyn beskriver ansvar och organisation avseende säkerhetsarbetet. De roller som beskrivs är kommunfullmäktige, kommunstyrelsen, kommundirektören, säkerhet- och beredskapsfunktionen samt medarbetare och förtroendevalda. Policyn beskriver även kommunens strategi samt grundläggande principer avseende säkerhet. Säkerhetspolicyn finns tillgänglig på kommunens intranät. Nyanställda får en genomgång av kommunens policyer och riktlinjer som en del av introduktionen. Däremot sker ingen kontinuerlig kommunikation av policy och riktlinjer till medarbetare och det finns ingen rutin för att säkerställa att medarbetare har tagit del av policy och riktlinjer avseende informationssäkerhet. Det bedrivs ett arbete inom kommunen för att se över samtliga styrdokument då det enligt intervjuade nyckelpersoner i dagsläget finns för många och man endast vill behålla de som anses vara meningsfulla. Kommunens säkerhetschef har i uppdrag att kontrollera efterlevnad av policy, riktlinjer och regelverk samt kontrollera eventuella brister i informationssäkerhetsarbetet. Vid tid för granskning har dock efterlevnad ej börjat att kontrolleras.	Det saknas en dokumenterad rutin för att säkerställa att kommunens medarbetare har kännedom om säkerhetspolicy och riktlinjer avseende informationssäkerhet. Det saknas en dokumenterad och implementerad metod för att kontrollera efterlevnad av policy och riktlinjer.	2,00
Strategi och rutiner	Kommunen har en säkerhetsstrategi som beskrivs i säkerhetspolicyn. Vidare har kommunen flertalet riktlinjer avseende IT- och informationssäkerhet, däribland riktlinje för konsekvensbedömning,		1,50

	informationshanteringsplan samt riktlinjer avseende dokumentation. Kommunen har en upprättad riktlinje som stipulerar att styrdokument årligen ska följas upp av dokumentansvarig och vid behov revideras. Det finns dock inget krav på dokumentation av uppföljning om ingen förändring av styrdokumentet sker och vid tid för granskning noterades att flertalet riktlinjer senast uppdaterades under 2019.	Kommunen har ej säkerställt att styrande dokument förblir riktiga och aktuella över tid.	
Organisation	Kommunens säkerhetschef samordnar informationssäkerhetsarbetet. Enligt intervjuad nyckelperson ligger kommunens ansvarshantering av informationssäkerhet hos respektive nämnd och förvaltningschef. Kommunstyrelsen har genomfört informationstillfällen med kommunens nämnder där säkerhetsskyddsarbetet har varit på agendan, dock utan specifikt fokus på informationssäkerhet. Informationstillfällena genomförs inte systematiskt och de är inte del av ett årshjul. Kommunstyrelseförvaltningen har en upprättad internkontrollplan för 2022. Dock innefattar denna inte IT- eller informationssäkerhet. Kommunen använder SKR:s avtalsmall för personuppgiftsbiträdesavtal (pub-avtal) med externa leverantörer av informationsbehandlingstjänster. Kommunens allmänna avtalsvillkor beskriver att leverantören förbinder sig att använda konfidentiell information enbart i syfte att fullgöra sina respektive åtaganden gentemot kommunen och inte för något annat ändamål.	Ingen specifik uppföljning av informationssäkerhetsarbetet genomförs av kommunstyrelsen.	1,75

2.2 Personal och behörigheter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personal och behörigheter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 4).

Tabell 4: Nuläge och iakttagelser inom huvudområdet Personal och behörigheter

Område	Nuläge	Iakttagelser	Mognad
Personal	Informationssäkerhet ligger inom Säkerhetschefens ansvarsområde tillsammans med övriga säkerhetsuppdrag. Enligt intervjuad nyckelperson finns det ett behov av att utöka resurserna inom informationssäkerhetsfunktionen. Vid tid för granskning bedrivs ett arbete för att anställa ytterligare person inom säkerhetsområdet, men enligt intervjuad nyckelperson ligger inte fokus på att anställa inom just informationssäkerhetsområdet.	Det finns ett uttryckt behov av att öka bemanningen kopplad till arbetet med informationssäkerhet.	1,80

	Vid nyanställning till kritiska roller avseende informationssäkerhet genomförs säkerhetsprövning. Nivån på säkerhetsprövningen beror på rollens behörighetsnivå. Enligt intervjuad nyckelperson har kommunen utsett systemägare för samtliga system som kommunen anser att det finns ett behov av. Eventuellt saknas systemägare för några mindre system. Kommunen har en lista över samtliga system. Utbildningar avseende IT-säkerhet för kommunens medarbetare planeras att påbörjas under 2022. Utbildningarna ska levereras av kommunens IT-bolag (samägt med Hörby kommun, Höörs kommun, Osby kommun och Östra Göinge kommun). Utbildningarna bygger på interaktiva nanoutbildningar och användare ska kontinuerligt testas genom utskick av test-mejl. Samtliga anställda inom kommunen genomgick en webbaserad informationssäkerhetsutbildning för två år sedan. Denna utbildning har ej följts upp av ytterligare utbildningstillfällen och vid tid för granskning har kommunen ingen plan för kontinuerlig utbildning avseende informationssäkerhet.	Det saknas en kontinuerlig och obligatorisk utbildningsplan avseende informationssäkerhet.	
Behörighets-hantering	I dokument från kommunens samägda IT-bolag beskrivs vissa roller avseende behörighetshantering, såsom att systemansvariga i verksamheterna styr behörigheter för åtkomst till informationen i system, medan IT styr åtkomst till systemen. Det finns däremot ingen dokumenterad riktlinje för tilldelning, förändring och avslut av användarbehörigheter till system. Enligt intervjuad nyckelperson ser processen för behörighetstilldelning olika ut beroende på hur systemet är tekniskt uppbyggt, där ansvaret kan ligga på antingen IT eller systemförvaltaren. Även behörigheter på infrastrukturell nivå tilldelas enligt olika processer beroende på system. Enligt intervjuad nyckelperson har kommunen använt olika metoder för att säkerställa att roller inom informationssystem är segregerade. En metod är att vid införandet av nya system ses behörigheter över för att identifiera vilka behörigheter som skulle kunna innebära en intressekonflikt. En annan metod är att det är inbyggt i de flesta systemen att personen som begär behörighet inte kan vara samma person som godkänner den. Trots ovan nämnda metoder har det inte genomförts någon utarbetad analys av roller inom organisation och system för att säkerställa att roller är lämpligt segregerade. Det finns heller inte någon dokumenterad styrning för hur roller bör vara segregerade för att undvika intressekonflikt. Behörigheter med åtkomst till infrastruktur kontrolleras månadsvis för att säkerställa att rätt	Det saknas en dokumenterad riktlinje förtilldelning, förändring och avslut av användarbehörigheter i system. Det saknas en dokumenterad riktlinje för tilldelning, förändring och avslut av användarbehörigheter på infrastrukturell nivå. Det saknas dokumenterad styrning för hur roller inom organisationen och system bör vara segregerade.	1,60

	person har rätt åtkomst. Vem som har genomfört kontrollen för vilka behörigheter dokumenteras i en arbetsbok. Det genomförs inte några periodiska genomgångar av behörigheter som inte är kopplade till infrastruktur.	Det saknas dokumenterade rutiner avseende periodiska genomgångar av behörigheter utan åtkomst till infrastruktur.	

2.3 Drift

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *drift* samt de iakttagelser som noterats under granskningens utförande (se Tabell 5).

Tabell 5: Nuläge och iakttagelser inom huvudområdet Drift

Område	Nuläge	Iakttagelser	Mognad
Incident-hantering	Kommunen har praktiska rutiner för hur informationssäkerhetsincidenter hanteras, men dessa är inte dokumenterade. Enligt intervjuade nyckelpersoner ska säkerhetssamordnare kontaktas för att hantera och diarieföra ärendet. Personen som rapporterar incidenten ska bli intervjuad av säkerhetssamordnaren för att finna rotorsak som sedan rapporteras till tillsynsmyndigheten. Informationssäkerhetsincidenter ska rapporteras till kommunstyrelsens arbetsutskott men rapporteringen är inte protokollförd.	Det saknas en dokumenterad riktlinje avseende hantering och dokumentation av informationssäkerhets-incidenter. Rapportering till kommunstyrelsens arbetsutskott protokollförs ej.	1,33
Informations-klassning	Informationsklassning är det första steget i kommunens riktlinje för riskanalys och beskriver risker som inträffa utifrån perspektiven konfidentialitet, riktighet, tillgänglighet och spårbarhet. Vid tid för granskning bedriver kommunen ett arbete för att informationsklassa samtliga system där samtliga förvaltningar är i slutfasen av informationsklassningarna och ska påbörja riskanalyser. I samband med registreringen av det gemensamma it-bolaget 2020 så genomförde kommunen ett arbete för att identifiera sina verksamhetskritiska informationssystem. Vilka av kommunens system som anses vara verksamhetskritiska har bedömts utifrån enskilda förvaltningars verksamheter, ej utefter centrala direktiv.	Kommunen har vid tid för granskning inte informationsklassat samtliga informationssystem. Kommunen har vid tid för granskning inte genomfört riskanalys för samtliga relevanta informationssystem. Det saknas centrala riktlinjer för vad som klassificeras som verksamhetskritiskt system.	1,50
Nätverk	Kommunens IT-miljö driftas i sin fullo av kommunens samägda IT-bolag som även ansvarar för nätverkssegmenteringen. Enligt dokumentation segmenteras nätverkstrafik efter behov identifierade av IT-bolaget, bland annat finns ett klientnätverk för personal, ett för elever och ett management-nätverk. Enligt intervjuad nyckelperson är både "intrusion detection system" och "intrusion prevention system implementerade" implementerade för att analysera nätverksaktivitet.	Det saknas kravställning gällande nätverksmiljön mot samägt IT-bolag.	2,00

Brandväggar	Kommunen har ingen brandväggspolicy eller dokumenterad riktlinje avseende hantering av brandväggar. Kommunen har dock praktiska rutiner för hur man arbetar med brandväggar och styr brandväggsrelaterade aktiviteter. Exempelvis får bara en person arbeta i brandväggen samtidigt. Granskning av brandväggarnas konfiguration sker inte regelbundet utan det har genomförts riktade insatser när avvikelser har identifierats. Rutinen är att det genomförs ett så kallat "städ-jobb" av avvikelsen så att denna åtgärdas.	Kommunen saknar dokumenterad policy eller riktlinje för att styra och kontrollera hanteringen av brandväggar. Det saknas en dokumenterad rutin avseende regelbunden granskning av brandväggarnas konfiguration.	1,00
Kontinuitetsplanering	Kommunens samägda IT-bolag har en dokumenterad definition av kris. Enligt intervjuad nyckelperson delar kommunen samma bild av vad som definieras som kris, men kommunen har ingen egen dokumentation för definition av kris/katastrof avseende informationssäkerhet. Kommunen tog fram en övergripande kontinuitetsplan under 2016. Kontinuitetsplanen blev dock inte beslutad och är således ej implementerad.	Det saknas dokumentation från kommunens sida avseende vad som definieras som en kris/katastrof avseende informationssäkerhet. Kommunen saknar en beslutad och implementerad kontinuitetsplan.	1,33

2.4 Programförändringar

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *programförändringar* samt de iakttagelser som noterats under granskningens utförande (se Tabell 6).

Tabell 6: Nuläge och iakttagelser inom huvudområdet Programförändringar

Område	Nuläge	Iakttagelser	Mognad
Förändrings-hantering	Kommunen har en dokumenterad process för programutveckling av operativsystemet Windows 10. För övriga informationssystem förs en dialog mellan systemförvaltare och leverantören vid programutveckling, men det finns ingen dokumenterad process för hur system- och programförändringar ska efterfrågas, utvecklas, testas och implementeras. Vid tid för granskning har kommunen ingen dokumenterad rutin eller riktlinje avseende hantering av patchningar. Enligt intervjuad nyckelperson uppdateras patchningar från Microsoft inom skälig tid och det sparas vilka patchningar som rullats ut och vilka som har blockerats.	Det saknas en dokumenterad rutin för hur programförändringar ska genomföras. Det saknas en dokumenterad rutin för hur patchningar ska hanteras.	1,33

2.5 Personuppgifter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personuppgifter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 7).

Tabell 7: Nuläge och iakttagelser inom huvudområdet Personuppgifter

Område	Nuläge	Iakttagelser	Mognad
Personuppgifts -styrning	Kommunen har en dataskyddspolicy som är beslutad av kommunfullmäktige under 2019. Policyn är giltig tills vidare och det har inte dokumenterats att den reviderats sedan dess. I dataskyddspolicyn framgår det att samtliga kommunens nämnder och bolag ska utse ett dataskyddsombud. I kommunens riktlinje avseende personuppgiftsbehandling beskrivs dataskyddsombudets roll och ansvar. Riktlinjen för personuppgiftsbehandling beskriver även kommunens övergripande arbete med personuppgiftshantering, vilket innefattar bland annat hur personuppgifter ska hanteras, hur personuppgiftsbiträden ska hanteras samt registrerades rättigheter. Riktlinjen för personuppgiftsbehandling beslutades 2019 och har antagits av samtliga nämnder. Revision av riktlinjen har ej dokumenterats. Det har inte dokumenterats att den reviderats sedan dess. Kommunen har utsedda GDPR-ombud som är ansvariga för dataskyddsfrågor i kommunens nämnder och förvaltningar. Kommunens dataskyddssamordnare sitter som centralt stöd i dataskyddsfrågor för kommunens GDPR-ombud. Kommunen har även ett externt dataskyddsombud från ett kommunalförbund. Kommunstyrelsen informeras vid förändringar i kommunens dataskyddsarbete, bland annat gällande vad förändringen är och vad de förväntade konsekvenserna är. Däremot efterfrågar inte kommunstyrelsen regelbunden rapportering gällande dataskyddsarbetet.	Kommunen har ej säkerställt att styrande dokument avseende dataskydd förblir riktiga och aktuella över tid. Det saknas en dokumenterad rutin för hur dataskyddsarbetet ska rapporteras till kommunstyrelsen.	2,00
Personuppgifts -behandling	Respektive nämnd i kommunen har varsin upprättad registerförteckning över personuppgiftsbehandlingar. Registerförteckningarna följer SKR:s mall och lever upp till kraven i dataskyddsförordningen. Vid tid för granskning har kommunen upphandlat ett nytt system som ska förenkla hanteringen av registerförteckning. Systemet ska implementeras under 2022. Kommunen skriver pub-avtal enligt SKR:s avtalsmall med leverantörer som hanterar kommunens personuppgifter. Pub-avtalen stipulerar att kommunen har rättigheten att granska leverantörens dataskyddsarbete. I undantagsfall tar leverantören fram ett pub-avtal som kan godtas ifall kommunen bedömer dem vara likvärdigt med SKR:s avtalsmall. Kommunen har inte följt upp att samtliga leverantörer lever upp till kraven i dataskyddsförordningen.	Kommunen har inte följt upp att leverantörer som hanterar kommunens information lever upp till krav i GDPR.	2,50

Personuppgifts -rutiner	Kommunen har en dokumenterad rutin för genomförande av riskanalys samt efterföljande konsekvensbedömning. Rutinen beskriver att riskanalys ska genomföras för samtliga personuppgiftsbehandlingar som kan innebära en risk för den enskildes rättigheter. Riskanalysen innebär att identifiera potentiella säkerhetsrisker med respektive personuppgiftsbehandling. Enligt rutinen ska en riskanalys genomföras för varje identifierad risk. Utifrån riskanalysen beslutas om en konsekvensbedömning ska genomföras. Enligt rutinen ska konsekvensbedömning genomföras för samtliga personuppgiftsbehandlingar med identifierad hög risk. Vid tid för granskning har kommunen ingen dokumenterad process för att säkerställa att riskanalys och konsekvensbedömning genomförs för samtliga relevanta personuppgiftsbehandlingar. Kommunen har en dokumenterad rutin för incidenthantering avseende dataskydd vilken stipulerar att identifierade eller misstänkta personuppgiftsincidenter ska rapporteras till närmsta chef utan dröjsmål, även om incidenten redan har åtgärdats. Berörd chef kontaktar därefter verksamhetens GDPR-ombud som bedömer incidentens allvarlighetsgrad och beslutar om vidare åtgärd. Personuppgiftsincidenten ska även dokumenteras i verksamhetens diarium. I dokumentationen beskrivs bland annat information kring händelsen, potentiella konsekvenser och åtgärder. Vid tid för granskning har kommunen ingen process för att säkerställa att rutinen efterlevs. Kommunen tog fram en informationshanteringsplan under 2021 som gäller för samtliga nämnder och verksamheter. Enligt intervjuad nyckelperson ska gallring och lagring av personuppgifter ske enligt dokumenthanteringsplanen. Vid tid för granskning finns det ingen dokumenterad rutin för att säkerställa att lagring och gallring av personuppgifter sker utefter dokumenthanteringsplan.	Det saknas en dokumenterad rutin för att säkerställa att riskanalys och konsekvensbedömning genomförs för samtliga relevanta personuppgiftsbehandlingar. Det saknas en dokumenterad process för att säkerställa att rutinen för personuppgiftsincidenter efterlevs i praktiken. Det saknas en dokumenterad process för att säkerställa att lagring och gallring av personuppgifter sker utefter dokumenthanteringsplan.	2,33
Dataskydd	Kommunen får årligen en sammanställning av åtgärdsförslag avseende dataskydd från kommunalförbundet. Förslagen baseras på en enkät med frågor om kommunens dataskyddsarbete som kommunens dataskyddssamordnare och GDPR-ombud svarar på.		3,00
Utbildning inom dataskydds-förordningen	Utbildning avseende dataskydd tillhandahålls av det externa kommunalförbundet som löpande håller grund- och vidareutbildningar. Utbildningarna inkluderar områden som bland annat organisation, ansvar och registerförteckning. Samtliga medarbetare uppmanas	Kommunen saknar en kontinuerlig och obligatorisk utbildningsplan avseende dataskydd.	2,00

	av kommunen att delta på utbildningarna men närvaro är inte obligatoriskt. Vid nyanställning upplyses den nyanställda om dataskyddsförordningen. Det har även hållits utbildningar avseende dataskydd i samband med chefsutbildningar, men framöver finns det ingen plan för att fortsätta genomföra dessa. Kommunen har ingen obligatorisk och kontinuerlig utbildningsplan avseende dataskydd som gäller för samtliga medarbetare som hanterar personuppgifter.		
Molntjänster	Kommunen hanterar personuppgifter i flertalet molntjänster. Vid upphandling av dessa molntjänster har kommunen tecknat pub-avtal med leverantören enligt SKR:s avtalsmall som reglerar kraven på molntjänstleverantören avseende personuppgiftshantering. Avtalen innefattar krav på att kommunens personuppgifter endast efter skriftligt godkännande från kommunen får hanteras och lagras utanför EU/EES. Ett undantagsfall är molntjänsten Microsoft 365 där personuppgiftshantering regleras i leverantörens standardavtal. Enligt intervjuad nyckelperson kan det finnas ytterligare molntjänster som används inom kommunen som inte är kända för kommunens samägda IT-bolag då det historiskt har hänt att verksamheter upphandlar molnsystem utan att meddela detta.	Det saknas en dokumenterad process för att säkerställa att upphandling av molntjänster kommuniceras till kommunens samägda IT-bolag.	2,00

3 Övergripande rekommendationer

Granskningen har identifierat iakttagelser inom flera delar av ramverket. EY har valt att presentera de mest relevanta rekommendationerna för Osby kommun och förslag på åtgärder för de främsta riskerna inom informationssäkerhetsarbetet.

Kontinuitetsplan

Vid tid för granskning saknar kommunen en beslutad kontinuitetsplan. Kommunstyrelsen rekommenderas tillse att en kontinuitetsplan upprättas, beslutas och implementeras. Detta för att säkerställa att kommunens verksamheter ska kunna verka och upprätthållas vid inträffande av störning, kris eller katastrof.

Styrande dokument

Vid tid för granskning saknar kommunen ett flertal relevanta styrdokument avseende IT- och informationssäkerhet. Kommunstyrelsen rekommenderas tillse att styrdokument upprättas och implementeras avseende områden såsom behörighetshantering, informationssäkerhetsincidenter, brandväggshantering och hantering av programförändringar. Därtill rekommenderas kommunstyrelsen tillse att en rutin upprättas och implementeras avseende att granskning av styrdokument ska dokumenteras även fast det inte sker någon uppdatering. Detta för att säkerställa att styrande dokument förblir riktiga och aktuella över tid.

Utbildningsplan

Vid tid för granskning saknar kommunen en plan för obligatoriska utbildningar avseende IT- och informationssäkerhet. Kommunstyrelsen rekommenderas tillse att en heltäckande utbildningsplan avseende IT- och informationssäkerhet upprättas och implementeras. Utbildningarna bör vara kontinuerliga och obligatoriska för samtliga medarbetare som hanterar kommunens information.

Internkontrollplan

Det sker ingen specifik rapportering till kommunstyrelsen avseende IT- och informationssäkerhet och det finns ingen definierad rutin för att säkerställa efterlevnad av styrande dokument. Kommunstyrelsen rekommenderas tillse att en internkontrollplan avseende IT- och informationssäkerhet upprättas som är heltäckande för samtliga områden inom kommunens IT- och informationssäkerhetsarbete. Genom en heltäckande internkontrollplan kan kommunstyrelsen kontrollera efterlevnad av policy och riktlinjer avseende IT- och informationssäkerhet samt upptäcka eventuella gap.

Kommunikation av styrdokument

Styrande dokument avseende IT- och informationssäkerhet finns tillgängliga på kommunens intranät. Däremot sker ingen kontinuerlig kommunikation till medarbetare och det finns ingen rutin för att säkerställa att medarbetare har tagit del av policy och riktlinjer avseende IT- och informationssäkerhet. Kommunstyrelsen rekommenderas tillse att en dokumenterad plan upprättas för kontinuerlig kommunikation av policy och riktlinjer avseende IT- och informationssäkerhet, både till nyanställda och samtliga medarbetare inom kommunen. Kommunikationsplanen bör även indikera vem som ansvarar för att kommunicera policy och riktlinjer till medarbetare inom kommunen.

Building a better working world

Ledningssystem för informationssäkerhet

Kommunen har inte implementerat något ledningssystem för informationssäkerhet. Kommunstyrelsen rekommenderas tillse att ett ledningssystem för informationssäkerhet upprättas och implementeras. Inspiration kan tas från material som tillhandahålls av MSB, SKR och även den svenska och internationella standardserien ISO/IEC 27000.

Bemanning inom informationssäkerhetsområdet

Kommunen har vid tid för granskning uttryckt ett behov av att öka bemanningen kopplad till informationssäkerhetsområdet. Kommunstyrelsen rekommenderas tillse att bemanningen kopplad till informationssäkerhetsområdet är tillräcklig för att kunna utföra det jobb de har givits mandat för, samt för att säkerställa att det finns tillräckligt med kompetenta resurser för att lämpligt behandla och hantera samtliga områden avseende informationssäkerhet.

4 Revisionsfrågor

Granskningen har utgått från revisionsfrågan: bedriver Osby kommun ett tillräckligt och ändamålsenligt IT- och informationssäkerhetsarbete? Revisionsfrågan har brutits ner och besvarats enligt nedan.

Tabell 8: Förklaring av färgkod

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvaras delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Tabell 9: Svar på revisionsfrågor

Revisionsfråga	Svar	
▸ Kan *styrningen* av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamheter har, bedömas som ändamålsenligt?	Styrningen av kommunens arbete med IT- och informationssäkerhet bedöms inte vara ändamålsenlig. Svaret grundar sig i nedan. Kommunen har inte ett implementerat ledningssystem för informationssäkerhet. Kommunen saknar även ett riktlinjer och rutinbeskrivningar inom ett flertal områden avseende informationssäkerhet, däribland utbildningsplan, behörighetshantering och brandväggspolicy. Därtill bedöms kommunen inte ha säkerställt en tillräcklig bemanning inom informationssäkerhetsområdet.	
▸ Är arbetet med att *följa upp* att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?	Uppföljningen av efterlevnad av kommunens arbete med IT- och informationssäkerhet bedöms inte vara ändamålsenlig. Svaret grundar sig i att det vid tid för granskning saknas en dokumenterad och implementerad metod för att kontrollera och säkerställa efterlevnad av policy och riktlinjer. Därutöver sker inte någon specifik rapportering eller uppföljning avseende informationssäkerhetsarbetet till kommunstyrelsen.	
▸ Är Osby kommuns *incidenthanteringsprocess* ändamålsenlig?	Kommunens incidenthanteringsprocess bedöms inte vara ändamålsenlig. Svaret grundar sig i att kommunen saknar en dokumenterad rutin eller riktlinje avseende	

	hantering och dokumentation av informationssäkerhetsincidenter. Kommunen har en dokumenterad riktlinje avseende personuppgiftsincidenter. För informationssäkerhetsincidenter saknas dokumenterade riktlinjer.	

5 Slutsatser

Granskningens syfte har varit att bedöma om det finns brister i kommunens interna kontroll avseende informationssäkerheten. Vidare har syftet också varit att bedöma i vilken omfattning kommunstyrelse och nämnder styr och följer upp detta arbete.

Baserat på den analys och granskning som genomförts bedöms Osby kommun ha en genomsnittlig mognadsgrad på 1,78 av 5,0 vilket är en markant lägre mognadsgrad än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,49. Mognadsgraden för Osby kommun är betydligt lägre än vad EY rekommenderar för en kommun likt Osby, givet den mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras. Granskningsresultatet indikerar att kommunens mognadsgrad är något högre avseende personuppgifter och lägre inom drift och programförändringar.

EY:s övergripande bedömning är att Osby kommuns arbete med IT- och informationssäkerhet inte är ändamålsenligt. Bedömningen grundar sig i att kommunen inte har ett implementerat ledningssystem samt saknar flertalet styrdokument avseende IT- och informationssäkerhet, bland annat kontinuitetsplan. Därtill saknar kommunen en dokumenterad och implementerad metod för att kontrollera efterlevnad av policy och riktlinjer samt kontinuerligt rapportera till kommunstyrelsen. Bedömningen grundar sig även i att kommunen saknar en dokumenterad rutin avseende hantering och dokumentation av informationssäkerhetsincidenter.

Med grund i ovan är EY:s främsta rekommendationer att kommunstyrelsen i Osby kommun tillser att:

- En kontinuitetsplan upprättas, beslutas och implementeras.
- Styrdokument upprättas och implementeras inom ett flertal identifierade områden avseende kommunens IT- och informationssäkerhetsarbete.
- En utbildningsplan upprättas avseende IT- och informationssäkerhet.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Stockholm 2022-06-09

Helena Törnqvist, Partner, EY

Bilaga 1: Källförteckning

Intervjuade roller:

- Administrativ chef
- Säkerhetschef/säkerhetsskyddschef
- Dataskyddssamordnare
- Konsult från kommunens samägda IT-bolag

Dokumentförteckning från kommunen:

- Allmänna avtalsvillkor
- Avtalsmall
- Beredskapsplan livsmedel och vatten
- Checklista för introduktion av nyanställd
- Dataskyddspolicy
- Formulär - informationsinventering samt Informationsklassning
- Handlingsplan Treserva- 2019-03-13
- Informationshanteringsplan Hälsa och Välfärd
- Informationshanteringsplan Osby kommun
- Informationssäkerhetsinstruktion Användare
- Informationssäkerhetsinstruktion Bilaga 1 Ansvarsförbindelse Osby kommun
- Informationssäkerhetsinstruktion Förvaltning
- Informationssäkerhetsinstruktion Kontinuitet
- Informationssäkerhetspolicy
- Intern kontrollplan 2022 – Kommunstyrelseförvaltningen
- Osby Kommunstyrelsen Enkätsvar Dataskyddsefterlevnad 2022
- Osby Verksamhetssystem
- Presentation Tillsyn Osby
- Registerförteckning Hälsa och välfärd
- Riktlinje dokumentation hälsa- och omsorgsnämnden
- Riktlinje Personuppgiftsbehandling
- Riktlinje social dokumentation
- Riktlinjer för informationssäkerhet
- Riktlinjer styrdokument
- Risk och konsekvensbedömning Alfa
- Riskverktyg
- Rutin Begäran om registerutdrag
- Rutin för gallring och utlämning av e-post
- Rutin för Krisstöd Arbete och välfärd
- Rutin hantering hemliga handlingar
- Rutin Incidenthantering Dataskydd
- Rutin Konsekvensbedömning Dataskydd
- Rutin Personuppgiftsbehandling
- Rutin Systemförvaltare 2019
- Stödmaterial och förhållningsregler dokumentation
- Säkerhetspolicy
- Säkerhetsskyddsplan

Dokumentförteckning från kommunens samägda IT-bolag:

- Bilaga 1 Definitioner
- Bilaga 2 Förteckning tjänster - Teknisk plattform
- Bilaga 3 Förteckning tjänster - IT-arbetsplats
- Bilaga 4 Förteckning verksamhetskritiska system
- Bilaga 5 Beskrivning ärendehantering ServiceDesk
- Bilaga 6 Backup- och återläsningsplan
- Bilaga 8 Beställning av ny tjänst
- Bilaga 9 SLA-bilagan
- Drift och hantering av tillgångar – Krisrutin
- Drift och hantering av tillgångar - Processbeskrivning incidenthantering - Rutin för hantering av virussmittad klient
- Drift och hantering av tillgångar -Rutin för information vid kris, utan kontaktvägar
- Huvudavtal
- Personal och åtkomst – Behörighetshantering
- Personal och Åtkomst – Lösenordspolicy
- Personal och Åtkomst - Utbildningsplan – Nimblr
- Personal och åtkomst - Åtkomst till infrastrutkur
- Programförändringar - Process Win10 Livscykel

Building a better working world

Bilaga 2: Definitioner

Dataskyddsombud (DSO): Särskilt utsedd person vilken tillser att personuppgifter behandlas på korrekt och lagenligt sätt inom organisationen, genom att till exempel utföra kontroller och utbildningsinsatser.

Informationsklassning: Klassning av informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet, tillgänglighet och konfidentialitet.

Informationssäkerhet: Säkerhetsfrågor som berör information, oberoende av system och plattformar.

Informationssäkerhetssamordnare: Särskilt utsedd person som innehar det övergripande ansvaret att leda och samordna utvecklingen av kommunens informationssäkerhet.

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurering.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

Ledningssystem: Definierat verktyg eller system för att leda, planera, kontrollera, följa upp och utvärdera den egna verksamhetens arbete med informationssäkerhet.

Molntjänster: Tjänster och system som inte drivs lokalt av kommunen och som nås via en internetuppkoppling och inte direkt via det lokala nätverket.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.

Patchning: Tillägg till ett program eller system avsett att rätta till sårbarheter.

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats, tex drift, support och förvaltning av systemet.

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.

Objektägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.