Svalövs kommun

Rapport: IT- & Informationssäkerhetsgranskning
November 2021

Sammanfattning

På uppdrag av Svalövs 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 (MBSs) styrningsmodell för offentliga organisationers IT- och informationssäkerhet, LIS.
- ISO/IEC 27000 standarden för informationssäkerhet
- God praxis och EYs erfarenhet inom IT-, Cyber – och informationssäkerhet.

Granskningen genomfördes under september till november 2021 och baserades på intervjuer med identifierade nyckelpersoner i kommunens IT- och informationssäkerhetsarbete och genomgång av insamlad styrdokumentation. Granskningen har byggt på EYs ramverk för granskning av IT- och informationssäkerhet, Granskningsprogram Cyber och Informationssäkerhet (GCI), särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 62 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive områdena. Representanter från kommunens IT- och informationssäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EYs utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Svalövs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en genomsnittlig mognadsgrad, med ett genomsnitt på 2,41 av 5.00, jämfört med jämförelsetalet 2,27. Detta är dock en lägre mognadsgrad än vad EY rekommenderar för en kommun likt Svalöv, givet den stora mängd information, och andel av känslig karaktär, som hanteras. Mognadsgraden bedöms vara som högst inom nätverk, förändringshantering och utbildning inom dataskyddsförordningen. Lägst anses mognadsgraden vara inom strategi och rutiner, samt personuppgiftsstyrning.

EY rekommenderar att Svalövs kommun förbättrar systematiken i deras IT- och informationssäkerhetsarbete, samt dokumenterar tydliga processer och riktlinjer kring hur arbetet med granskning och uppföljning ska genomföras. Detta inkluderar både efterlevnad av styrdokument, samt tredjeparters efterlevnad av på förhand definierade säkerhetskrav. Kommunen bör också säkerställa att arbetet med personuppgiftsstyrning sker på ett ändamålsenligt sätt, vilket inkluderar att ta fram saknade rutiner och att tillse att arbetet sker i enlighet med definierade styrdokument och gällande lagstiftning. Slutligen bör kommunen också säkerställa att styrdokument, och tillhörande riktlinjer, gällande IT- och informationssäkerhet förblir riktiga och aktuella över tid.

Innehållsförteckning

1. Bakgrund

Svalövs kommun och dess olika nämnder och förvaltningar hanterar stora mängder digital information. 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 IT- och informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

I sin årliga risk- och konsekvensanalys har kommunens revisorer identifierat risker relaterat till kommunens övergripande arbete med informationssäkerhet samt IT-risker kopplat till verksamhetskritiska system inom kommunen. Revisorerna har därför valt att genomföra en granskning för att kartlägga kommunens arbete med IT- och informationssäkerhet. Riskerna inom dessa områden är inte specifikt relaterade till Svalövs kommun utan gäller hela den offentliga sektorn.

En granskning av IT- och informationssäkerhet i Svalövs kommun har ej genomförts tidigare. Denna granskning avser ge en uppdaterad lägesbild kring hur arbetet med IT- och informationssäkerhet fortskrider.

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 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 styrningsdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?
- Är Svalövs 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 Svalövs kommun bedriver på central nivå. Intervjuer har endast utförts med representanter på central nivå och inte med representanter i förvaltningarna. 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 EYs 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. Information kring områdena har insamlats både genom granskning av relevanta dokument,

samt genom att EYs specialister genomför granskningsmöten med relevanta personalkategorier i kommunen.

Inledningsvis granskades relevant dokumentation kring kommunens rutiner och processer av EY. Därefter hålls granskningsmöten med kommunens representanter för att gå igenom de områden som är inkluderade i EYs 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 analyserades och bedömdes den samlade bilden av dokumentation samt information inhämtad via granskningsmöten.

Under granskningen har följande personer intervjuats:

- Team lead IT
- Driftchef IT
- Enhetschef Kansli
- Dataskyddsombud
- Trygghets- och säkerhetschef
- IT Chef

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

1.3.1 Bedömning avseende sammanfattande betyg av informationssäkerhetsarbete

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 Svalövs Kommuns mognadsgrad inom informationssäkerhetsområden

1	Saknas helt / fungerar mycket bristfälligt utan rutiner
2	Existerar men har inte formellt definierats / fungerar bristfälligt utifrån begränsade rutiner
3	Har definierats med delvis efterlevnad / fungerar godtagbart utifrån definierade rutiner
4	Har definierats och förvaltas med god efterlevnad / fungerar väl utifrån definierade rutiner
5	Har definierats och förvaltas med mycket god efterlevnad / fungerar optimalt utifrån mycket väl definierade rutiner

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. 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.

1.3.2 Tidsplan

Tidsplanen för arbetet såg ut enligt följande:

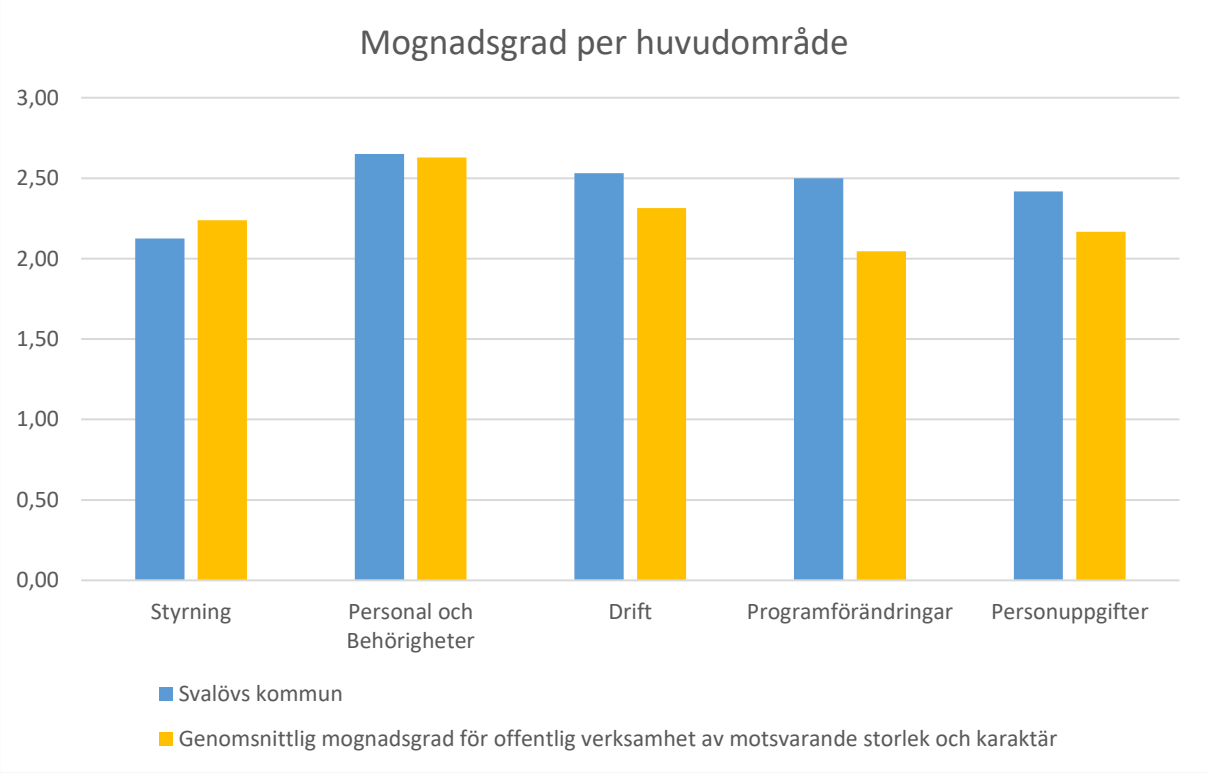
Förberedelser och planering	September 2021
Insamling och analys av dokumentation	September 2021
Arbetsmöte	September 2021
Rapportskrivning samt intern kvalitetssäkring	Oktober 2021
Faktagranskning av kommunen	November 2021
Justering samt färdigställande av rapport	November 2021
Avrapportering och slutpresentation	November 2021

2. Analys

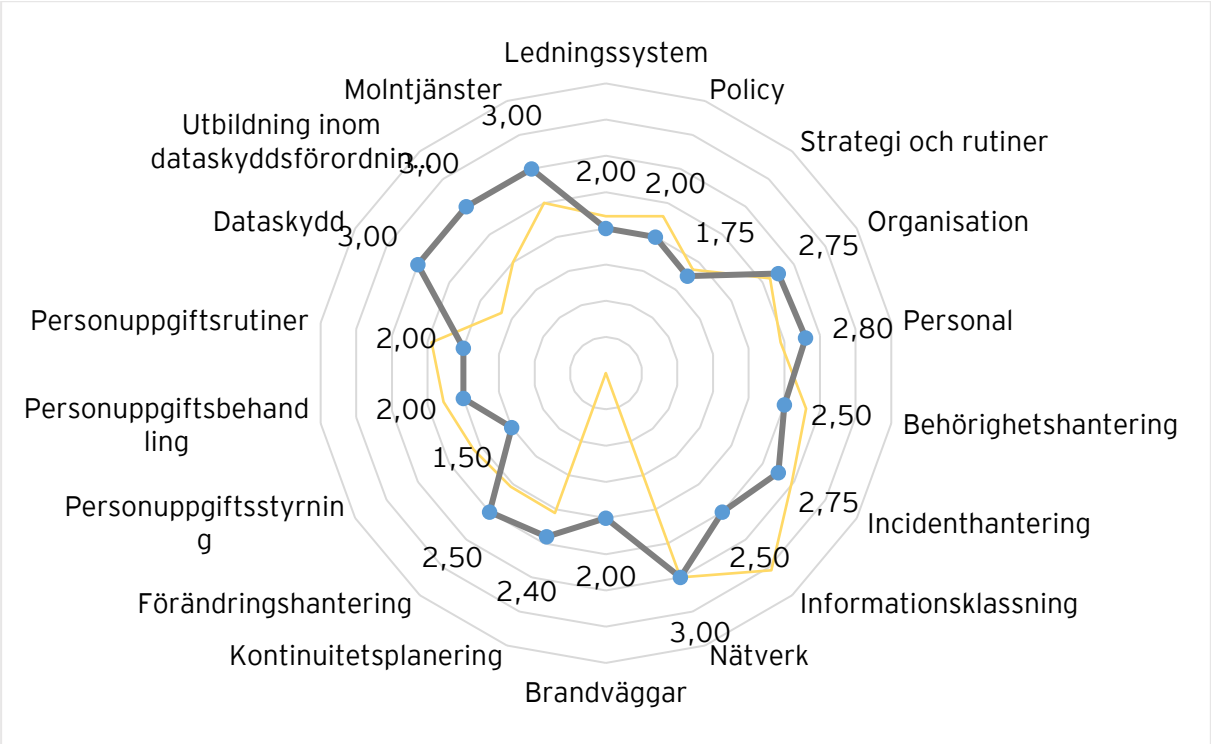
Baserat på den analys och granskning som genomförts bedöms Svalövs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en genomsnittlig mognadsgrad, med ett genomsnitt på 2,41 av 5,00, jämfört med jämförelsetalet 2,27. Detta är dock en lägre mognadsgrad än vad EY rekommenderar för en kommun likt Svalövs, givet den stora mängd information, och andel av känslig karaktär, som hanteras. Bilden nedan (figur 1) redovisar kommunens mognadsgrad för de 5 huvudområden som granskats, samt nedbrutet på 18 underområden (figur 2). Mognadsgraden bedöms vara som högst inom nätverk, förändringshantering, och utbildning inom dataskyddsförordningen. Lägst anses mognadsgraden vara inom strategi och rutiner, samt personuppgiftsstyrning.

Kommunens representanter har under granskningen påvisat kunskap och ambition inom informationssäkerhetsarbetet. Kommunen har också identifierat ett flertal områden med förbättringsbehov och redan påbörjat arbetet med att förbättra dessa. Ett exempel på detta är att kommunen under 2021 har implementerat en omfattande plan angående utbildning, exempelvis i form av e-learnings och medvetenhetstester.

Kommunens uppvisar ett förbättringsbehov inom strategi och rutiner, exempelvis genom att minska personberoenden och att aktivt arbeta med uppföljning och granskning. Kommunen uppvisar även ett behov av att förbättra arbetet med personuppgiftsstyrning, samt att säkerställa att styrdokument förblir riktiga och aktuella över tid.



Figur 1 – Överblick över kommunens mognadsgrad för de fem huvudområden som granskats i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär (gula staplar).



Figur 2 – Överblick över kommunens mognadsgrad för de fem huvudområden som granskats nedbrutet på 18 underområden i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär (gul linje).

2.1 Styrning

I sektionen nedan beskrivs nulägesbilden för huvudområdet *styrning* samt de iakttagelser som noterats under granskningens utförande (se Tabell 2).

Tabell 2: Nuläge och iakttagelser inom huvudområdet Styrning

Område	Nuläge	Iakttagelser	Mognad
Ledningssystem	Svalövs kommuns övergripande arbete med informationssäkerhet är inspirerat av principerna från ISO 27001. Kommunen arbetar dock inte strukturerat och enhetligt utefter ISO27001 eller något annat Ledningssystem för informationssäkerhet (LIS). Detta innebär att kommunen saknar ett definierat verktyg eller system för att leda, planera, kontrollera, följa upp och utvärdera den egna verksamhetens arbete med informationssäkerhet. Kommunen har dock tagit fram flertalet riktlinjer, rutiner och andra styrdokument som bidrar till att styra och följa upp arbetet med informationssäkerhet. Svalövs kommun har som en del i arbetet med att ta fram en digitaliseringsstrategi också tagit fram internt material för att kommunicera hur olika styrdokument för informationssäkerhetsarbetet hänger ihop och hur det kontinuerliga arbetet är upplagt.	Kommunen arbetar inte strukturerat utefter ett ledningssystem för informationssäkerhet.	2,0
Policy	Svalövs kommuns arbete med informationssäkerhet beskrivs på en övergripande nivå i den nuvarande		2,0

	informationssäkerhetspolicyn som fastslogs 2015. Informationssäkerhetspolicyn fungerar som det överordnade och styrande dokumentet. Nyanställda får ta del av informationssäkerhetspolicyn vid anställning och kommunens medarbetare kan nå informationssäkerhetspolicyn via intranätet. Enligt Svalövs kommuns befintliga informationssäkerhetspolicy skall policyn, instruktioner och riskanalyser ses över vid varje mandatperiod eller vid behov. Informationssäkerhetspolicyn har dock inte uppdaterats sedan 2015 och i dagsläget saknas fungerande rutiner för säkerställande av relevans och uppdatering. Policyn för informationssäkerhet är omfattande och inkluderar informationssäkerhetsinstruktioner för förvaltning, drift och användare. Det är således oklart huruvida informationssäkerhetspolicyn bör klassificeras som en policy eller en riktlinje.	Informationssäkerhetspolicyn samt tillhörande riktlinjer granskas och uppdateras med en för låg frekvens för att förbli aktuella. Kommunen har en delvis ostrukturerad dokumentklassificering relaterat till informationssäkerhet.	
Strategi och rutiner	Svalövs kommuns arbete med styrande dokument inom informationssäkerhet grundas i den övergripande policyn för informationssäkerhet. Policyn bryts sedan ner i mer specifika instruktioner för olika områden. I dagsläget finns det inga riktlinjer som länkar samman policyn med de specifika instruktionerna. Det existerar inte heller en informationssäkerhetsstrategi som definierar målsättningar för arbetet med informationssäkerhet på lång och kort sikt. Svalövs kommun har definierat ett antal olika instruktioner, eller rutinbeskrivningar, relaterat till informationssäkerhet. Några av dessa instruktioner och rutiner beskrivs mer nedan. Kommunen har under 2021 tagit fram en dokumenterad granskningsplan för att säkerställa att dokumenterade rutiner och instruktioner efterlevs i praktiken. Då planen nyligen har tagits fram har det inte skett någon strukturerad uppföljning på att policys och rutiner efterlevs i praktiken. I Svalövs kommuns *"Informationssäkerhetsinstruktion för Förvaltning"* har kommunen definierat generella regler gällande förteckning av tillgångar. Regler och riktlinjer för åtkomst till informationssystem beskrivs både i *"Informationssäkerhetsinstruktion för Användare"* och *"Informationssäkerhetsinstruktion för Drift"*. IT-incidenthantering samt säkerhetskopiering och lagring beskrivs i instruktionen för användare respektive drift. I *"Informationssäkerhetsinstruktion för Användare"* beskrivs även regler och riktlinjer för användning av dator, program, lösenordshantering, utrustning, distansarbete, hantering av lagrad/sparad digital information, användning av e-post och internet och avslut av anställning.	Kommunen saknar i dagsläget specifika riktlinjer och strategier för att leda det kortsiktiga och långsiktiga arbetet med informationssäkerhet. Det har ej genomförts någon strukturerad uppföljning på att definierade policys och rutiner efterlevs i praktiken.	1,75

Organisation	Hur Svalövs kommun har organiserat sitt arbete med informationssäkerhet beskrivs i kommunens informationssäkerhetspolicy och tillhörande informationssäkerhetsinstruktioner för förvaltning, användare och drift. Enligt den nuvarande policyn är det kommunfullmäktige som fastställer policyn och kommunchefen som har det övergripande ansvaret för att kommunens sektorer efterlever den. Systemägaren har det huvudsakliga ansvaret för informationssäkerheten i ett system och systemförvaltaren ansvarar för daglig drift och förvaltning. Under granskningen framkom det att definierade roller med tillhörande ansvar inte alltid efterlevs i praktiken. Det är exempelvis ibland oklart vem som har det operationella ansvaret att genomföra vissa uppgifter. Varje nämnd och styrelse skall utse ett dataskyddsombud och varje verksamhet ska ha en dataskyddssamordnare. Dataskyddsombudets huvudsakliga uppgift är att övervaka att kommunen följer dataskyddslagstiftningen genom att: - Samla in information om hur kommunen behandlar personuppgifter - Kontrollera att kommunen följer bestämmelser och interna styrdokument - Informera och ge råd inom kommunen I dagsläget ansvarar även dataskyddsombudet för att ta fram nya policys och riktlinjer. Kontroll av efterlevnad görs inte i nuläget, men det har gjorts tidigare. Innan oktober 2020 ansvarade en annan person för granskningsrollen. Enligt informationssäkerhetspolicyn ansvarar IT-chefen för att systemsäkerhetsanalys för teknisk IT-infrastruktur upprättas och hålls aktuell. Systemägaren och systemförvaltaren för respektive system ansvarar för att följa upp och delta i informationssäkerhetsarbetet i dialog med kommunens IT-funktion. Driftansvarig IT skall ge stöd till systemägare och systemförvaltare vid upprättande av systemsäkerhetsanalyser samt ansvara för att reservrutiner och serviceavtal finns för den grundläggande IT-infrastrukturen. Under granskningen framkom det att kommunen upprättar inträdesavtal med alla nya systemleverantörer för att säkerställa att de lever upp till kommunens säkerhetskrav. Kommunen håller även möten med de flesta leverantörerna och utför skanningstester för att säkerställa att systemen uppfyller kommunens säkerhetskrav. Någon gång under de senaste tre åren ska alla verksamheter ha kontrollerat att befintliga leverantörer lever upp till kraven och att inträdesavtal finns på plats. Det saknas dock en dokumenterad rutin för att regelbundet	Delar av den definierade organisationen och ansvarsfördelningen inom arbetet med informationssäkerhet efterlevs inte i praktiken. Det saknas i dagsläget en tydlig ansvarsfördelning inom kommunen som säkerställer att arbetet med personuppgifter kan bli oberoende granskat. Det saknas en dokumenterad rutin för att granska leverantörers efterlevnad av kommunens säkerhetskrav.	2,50

	granska leverantörer och på så sätt säkerställa att de lever upp till kommunens definierade säkerhetskrav.		

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 3).

Tabell 3: Nuläge och iakttagelser inom huvudområdet Personal och behörigheter

Område	Nuläge	Iakttagelser	Mognad
Personal	Enligt *"DATASKYDDSPOLICY – interna riktlinjer för hantering av personuppgifter"* från 2019 ska samtliga anställda erbjudas grundläggande dataskyddsutbildning. Enligt *"Utbildning inom dataskyddsområdet"* från 2021 framgår det att samtliga anställda har erbjudits obligatorisk utbildning inom GDPR och informationssäkerhet i form av e-learning med start i december 2020. Två efterföljande fördjupningsutbildningar inom samma tema kommer påbörjas under andra halvåret 2021. Enligt intervjuade nyckelpersoner är planen att fortsätta med e-learnings och göra uppföljning på grundkurserna. Cirka 80% av de anställda ska ha slutfört utbildningen. Under hösten 2021 kommer en ny utvecklingsplattform lanseras med regelrätta utbildningar och nanoutbildningar. I samband med introduktionen av GDPR 2018 erbjöds också en övergripande utbildning till utvalda delar av kommunen. Historiskt sätt har det dock ej genomförts regelbundna och årliga utbildningsinsatser inom informationssäkerhet. Svalövs kommun har nyligen tecknat avtal med en extern aktör för att varje kvartal genomföra säkerhetsmedvetentester i form av phishing-övningar. En sammanställning av resultatet skickas till ledningsgrupp och andra intressenter. Kommunen har genomfört en övning det senaste året men kommer framöver att öka frekvensen till varje kvartal. Enligt intervjuer med nyckelpersoner ska kritiska IT-befattningar placeras i säkerhetsklass och personal säkerhetsprövas. Säkerhetsprövning i form av intervjuer och registerkontroller ska således ske löpande samt vid nyanställning.	Kommunen har ej genomfört planlagda och årliga utbildningsinsatser inom informationssäkerhet.	2,8
Behörighets-hantering	Svalövs kommuns informationssystem är utrustade med ett behörighetskontrollsystem. Vilka behörigheter en användare tilldelas beror på dess arbetsuppgifter. Behörigheter beställs av respektive användares chef eller ansvarig systemförvaltare. Enligt intervjuade nyckelpersoner ansvarar förvaltningen för behörighetskontroll för de system		2,5

	som har systemförvaltare. IT-funktionen ställer krav på att verksamheterna går igenom behörigheter löpande och behörigheter ska granskas var tredje månad. Det saknas dock en dokumenterad rutin som inkluderar en tydlig kravställning samt beskrivning på hur denna genomgång ska genomföras. Enligt intervjuade nyckelpersoner sker avslut av anställning först via HR centralt, därefter är det chefens ansvar att anmäla avslut av användarbehörigheter. Avslut av nätverks- och e-postkonton anmäls till Helpdesk och avslut av behörigheter till verksamhetssystem anmäls till respektive systemförvaltare. I dagsläget händer det att vissa behörigheter inte avslutas vid avslut av anställning. Svalövs kommuns lösenordspolicy är dokumenterad i *"Informationssäkerhetsinstruktion för Användare"* och har följande krav: - Vara minst åtta tecken - Bestå av en blandning av stora (versaler) och små (gemener) bokstäver och siffror - Ska inte återanvändas Byte av lösenord för det interna nätverket sker var 90:e dag, men för enskilda program och system bestäms tidsintervall av respektive systemägare.	Kommunen saknar en dokumenterad rutin för periodiska genomgångar av behörigheter till kommunens informationssystem.	

2.3 Drift

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

Tabell 4: Nuläge och iakttagelser inom huvudområdet Drift

Område	Nuläge	Iakttagelser	Mognad
Incident-hantering	Enligt *"Informationssäkerhetsinstruktion för Förvaltning"* har driftansvarig IT ansvar för att rutiner för incidenthantering upprätthålls. Incidenter, eller misstänkta incidenter, ska omgående rapporteras till Helpdesk och berörd systemförvaltare. Det är också viktigt att rapportera allvarliga incidenter i nätverk och/eller verksamhetssystem till ansvarig chef. Alla incidenter ska registreras i ett ärendehanteringssystem. Helpdesk ansvarar därefter för att ta emot felanmälan, registrera ärendet och lösa eller överlämna ärendet till annan resurs med särskild kompetens. Incidenter loggas i kommunens system för rapportering, där kommunen har moduler för bland annat personuppgiftsincidenter och utredningar. Enligt intervjuade nyckelpersoner ska bevis för respektive		2,75

	incident samlas in och sparas i den mån det är möjligt. Enligt kommunen ska IT-personal ha tillgång till mer rutiner för hantering av incidenter och rutinerna är desamma oavsett om incidenten är relaterad till informationssäkerhet eller ej. Enligt intervjuade nyckelpersoner kan anställda anmäla personuppgiftsincidenter via ett applikationsfönster på datorn. Den efterföljande processen beror på hur verksamheten har lagt upp det, men ett vanligt upplägg är att ett meddelande skickas till dataskyddssamordnaren som i sin tur sätter ihop en utredningsgrupp. Riktlinjer för anmälan av personuppgiftsincidenter finns beskrivet i *"Riktlinjer för anmälan av personuppgiftsincidenter enligt dataskyddsförordningen"* från 2020. Varje verksamhet har egna rutiner för hantering av personuppgiftsincidenter, vilka uppdaterades 2021. Enligt de intervjuade ska incidenter alltid rapporteras till ledningsgruppen efter utförd utredning. Det saknas dock en dokumenterad process för att följa upp incidenthanteringsprocessen och säkerställa att den efterlevs. Angående incidenter som berör tredje part så har leverantörer enligt intervjuade nyckelpersoner en skyldighet att informera kommunen om incidenter, vilket regleras i systemavtalet. Därefter är det upp till berörd verksamhet att utvärdera incidenten vidare. Det är oftast den berörda verksamheten som meddelas om incidenten och det är således inte säkert att det förmedlas vidare till andra parter inom kommunen. Enligt kommunen har det under året inträffat en incident där den berörda verksamheten hanterade ärendet helt själva utan att informera kommunen om det inträffade. Kommunen har inte fått vetskap om någon dataläcka kopplat till incidenten.	Kommunen har ingen dokumenterad rutin över hur incidenthanteringsprocessen ska granskas. Kommunen har inte säkerställt tillräcklig spårbarhet genom incidenthanteringsprocessens hela livscykel.	
Informations-klassning	Enligt informationssäkerhetspolicyn sker klassificering med avseende på säkerhetsaspekterna sekretess, riktighet och tillgänglighet. Tre kravnivåer finns dokumenterade: mycket hög nivå, hög nivå och basnivå. Det finns hanteringsregler för respektive sekretessnivå och åtgärder i termer av förvaring, kopiering, återanvändning och destruktion. Åtgärder för att uppfylla säkerhetskraven för respektive system ska framgå av systemsäkerhetsplanerna. IT-chefen ansvarar för att systemsäkerhetsanalyser upprättas och hålls aktuella. Driftansvarig IT ansvarar för att stödja systemägaren och systemförvaltaren vid upprättande av systemsäkerhetsanalyser. Enligt intervjuade nyckelpersoner har kommunen beslutat om		2,5

	att se över sin informationsklassning och systemet som används för det. Riskanalyser ska enligt informationssäkerhetspolicyn utföras för alla förtecknade informationssystem som betraktas som samhällsviktiga och analyserna ska ses över vid varje mandatperiod eller vid behov. Enligt intervjuade nyckelpersoner hanteras arbetet med riskanalyser och riskhantering på olika sätt inom olika verksamheter. Vilka som utför riskanalyser och hur ofta de utförs varierar, men det ska enligt kommunen ske på löpande basis. Alla analyser dokumenteras dock inte. Kommunen ska ha beslutat om att ta fram övergripande och gemensamma bedömningsgrunder för att införa mer systematik i riskbedömningsprocessen. Kommunens representanter beskrev exempelvis att det inte utförs någon systematisk genomgång eller uppdatering av analyserna. Enligt Svalövs kommuns *"Riktlinjer för arkivvård och informationsförvaltning"* ansvarar respektive verksamhet för att i samråd med arkivmyndigheten upprätta, vårda och besluta om sitt arkiv samt att upprätta en dokumenthanteringsplan för den egna verksamheten. Dokumenthanteringsplanen ska bland annat innehålla anvisningar om rensning och gallring. Planen ska struktureras utifrån beslutad klassificeringsstruktur och är ett redskap för att ta fram rutiner för hantering av handlingar. De senast uppdaterade rutinerna är från 2020, men ett flertal är från 2018 eller tidigare. Klassificeringsstrukturen ska uppdateras löpande. Beskrivningar av arkiv och handlingar ska uppdateras löpande i samband med verksamhetsförändringar och rensning ska genomföras av ansvarig handläggare. Vid gallring ska gallringsprotokoll upprättas och diarieföras, men i dagsläget saknar vissa verksamheter diarieförda gallringsprotokoll på verkställd gallring. Dokument och handlingar ska lagras i kommunens arkivstruktur. Arkivläggning ska ske årligen, det vill säga att handlingar vars gallringsfrist har löpt ut ska hanteras årligen. Varje verksamhet kan ha egna rutiner för individärenden.	Kommunen har en delvis ostrukturerad process för hantering av risk- och sårbarhetsanalyser. Riktlinjer för arkivvård och informationsförvaltning efterlevs inte i praktiken.	
Nätverk	Enligt intervjuade nyckelpersoner har Svalövs kommun segregerat informationssystemen för respektive verksamhet och segregerat osäkra nät från säkra nät. Ingen obehörig har fysisk tillgång till nätverken och de nätverk som inte längre används stängs ned. Svalövs kommun ska även ha implementerat "intrusion detection system" (IDS) och "intrusion prevention system" (IPS). IDS och IPS är metoder för att analysera nätverksaktivitet. Detta genom att leta efter kända signaturer i nätverkstrafiken, samt att undersöka, och eventuellt stoppa, paket som försöker levereras över nätverket. Det finns ett system som konstant		3,0

	övervakar brandväggen och ett som tunnlar all aktivitet.		
Brandväggar	Enligt intervjuade nyckelpersoner har Svalövs kommun ingen dokumenterad brandväggspolicy. Kommunen har full kontroll över ett externt system som testar brandväggar och dess säkerhet genom penetreringstester från både insidan och utsidan på veckobasis. De flesta brandväggsreglerna ska enligt de intervjuade finnas dokumenterade men det finns ingen rutin för att regelbundet granska brandväggens konfiguration. Enligt intervjuade nyckelpersoner förekommer det leverantörer som använder standardportar som inte bör användas, vilket kommunen åtgärdar genom att stänga ned de berörda portarna.	Svalövs kommun har ingen dokumenterad brandväggspolicy eller dokumenterade rutiner för att regelbundet granska brandväggars konfiguration.	2,0
Kontinuitetsplanering	Svalövs kommun ska enligt informationssäkerhetspolicyn ha en kontinuitetsplan baserad på informationssystemens samlade krav och vara integrerad med kommunens gemensamma kontinuitetsplan. Enligt intervjuade nyckelpersoner finns det dock ingen dokumenterad kontinuitetsplan för arbetet med informationssäkerhet. Mycket av arbetet är individberoende och sker per automatik men är varken dokumenterat eller strukturerat som en formell process. Detta innebär att det saknas dokumentation för planering och åtgärder som syftar till att motverka avbrott och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer. Enligt de intervjuade har kommunen påbörjat ett arbete för att se över hur de kan minska sitt individberoende. Det ska enligt intervjuade nyckelpersoner finnas en reservplan över hur kommunen ska agera vid avbrott. Planen finns fysiskt i serverummet men är inte tillgänglig digitalt. Den beskriver vilka system som ska prioriteras och i vilken ordning som återställning ska ske. Planen uppdateras inte regelbundet men ses över i samband med systemförändringar. Det ska även bedrivas en kontinuerlig dialog med verksamheterna gällande systemen och en årlig diskussion gällande vilka system som är viktigast. Enligt intervjuade nyckelpersoner kontrolleras underhållsavtal för server och infrastruktur en gång om året. Teknisk infrastruktur och backup fungerar men det saknas regelbunden utvärdering och testning för återställning.	Det saknas en dokumenterad kontinuitetsplan för kommunens informationssystem. Kommunen har ingen dokumenterad rutin för att genomföra testning av IT-relaterade kontinuitets- och krisplaner.	2,40

2.4 Programförändringar

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

Tabell 5: Nuläge och iakttagelser inom huvudområdet Programförändringar

Område	Nuläge	Iakttagelser	Mognad
Förändrings-hantering	Enligt informationssäkerhetspolicyn ansvarar systemförvaltaren för att påtala eventuellt behov av förändringar till systemägaren som i sin tur ansvarar för att besluta om eventuella förändringar. Kommunen har dock ingen formellt dokumenterad programförändringsprocess och eventuella rutiner skiljer sig åt beroende på organisation och teknisk nivå. Enligt intervjuade nyckelpersoner kan tillvägagångssättet för att besluta om systemförändringar variera från fall till fall, men när ett behov av en förändring har påtalats inleds ofta en dialog mellan systemförvaltare, leverantör och IT. Om förändringen är verksamhetspåverkande anordnas workshops för att utvärdera huruvida en förändring uppfyller det tilltänkta målet. Arbete med patchningar utförs månatligen enligt ett fast schema. När rekommenderade patchningar släpps utvärderas möjligheten att lägga på dem direkt och i de fall patchningar inte kan genomföras direkt diskuteras andra lösningar. Det finns även ett system som loggar och hanterar vilka patchningar som har genomförts och vilka som inte har det.	Det saknas en dokumenterad rutin för arbetet med förändringar i kommunens IT-system.	2,5

2.5 Personuppgifter

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

Tabell 6: Nuläge och iakttagelser inom huvudområdet Personuppgifter

Område	Nuläge	Iakttagelser	Mognad
Personuppgifts-styrning	Svalövs kommuns *"DATASKYDDSPOLICY – interna riktlinjer för hantering av Personuppgifter"* är verksamhetsövergripande och uppdaterades 2019. Mer detaljerade riktlinjer finns beskrivna i *"Hantering av personuppgifter i Svalövs kommun"* från 2018. Dessa riktlinjer är gemensamma för hela kommunen och beskriver bland annat hantering av epost, personnummer och publicering av personuppgifter på hemsidan. Lokala riktlinjer gällande hantering av personuppgifter finns ej, men respektive verksamhet har egna rutiner för hantering av personuppgiftsincidenter. I nuläget finns dock ingen	Kommunen har inte uppdaterat styrdokument relaterat till personuppgiftsstyrning i en tillräckligt hög frekvens. Kommunen saknar vissa dokumenterade styrdokument	1,5

	formell process för att regelbundet granska och säkerställa efterlevnad av kraven i dataskyddsförordningen. Varje nämnd och styrelse är personuppgiftsansvarig för respektive verksamhet och skall utse ett dataskyddsombud vars uppgift är att övervaka och kontrollera att verksamheten följer dataskyddslagstiftningen vid behandling av personuppgifter. Dataskyddsombudet är också kontaktperson för Integritetsskyddsmyndigheten (IMY).	inom arbetet med personuppgiftsstyrning.	
Personuppgifts-behandling	Kommunen använder sig av ett system för att upprätthålla en registerförteckning för behandling av personuppgifter. Förteckningen avser att uppfylla artikel 30 i dataskyddsförordningen och ska administreras och löpande uppdateras av respektive verksamhet. Förteckningen ska fungera som ett heltäckande register över alla personuppgiftsbehandlingar i kommunen, men i dagsläget saknas uppdaterade förteckningar för ett flertal av kommunens verksamheter. Skriftliga personuppgiftsbiträdesavtal (PUB-avtal) ska tecknas med samtliga leverantörer och personuppgiftsbiträden vid behandling av personuppgifter. Personuppgiftsansvarig ansvarar för att se till att skriftliga PUB-avtal finns. Hur efterlevnad av avtalen säkerställs framgår ej och baserat på registerförteckningen verkar anställda vara osäkra på huruvida det finns rutiner för kontroll och revision av personuppgiftsbiträden.	Kommunen saknar en dokumenterad rutin för att följa upp och säkerställa att registerförteckningar är uppdaterade och kompletta över tid. Kommunen saknar en dokumenterad rutin för att säkerställa efterlevnad av ingångna PUB-avtal.	2,0
Personuppgifts-rutiner	År 2020 upprättade kommunen *"Riktlinjer för anmälan av personuppgiftsincidenter enligt dataskyddsförordningen"* och sedan 2021 har respektive verksamhet egna uppdaterade rutiner för hantering av personuppgiftsincidenter. Upptäckt eller misstanke om personuppgiftsincidenter ska rapporteras till personuppgiftsansvarig för bedömning av risker och eventuell anmälan till IMY. I *"Riktlinjer för anmälan av personuppgiftsincidenter enligt dataskyddsförordningen"* framgår vilka uppgifter som ska lämnas till registrerade samt vilka uppgifter som en anmälan till IMY ska innehålla. Det är den personuppgiftsansvariga för den verksamhet i vilken en incident har uppkommit som ansvarar för att en anmälan görs. Incidenter ska dokumenteras oavsett om de anmäls eller ej. Kommunen har dokumenterade riktlinjer för hantering av registerutdragsförfrågningar från registrerade och en lista över registrerades rättigheter. Dessa riktlinjer beskrivs i *"Hantering av personuppgifter i Svalövs kommun"* från 2018 och behandlar utdragets innehåll, format och tidsfrist. Svalövs kommun har utsett rollen som dataskyddsombud till kontaktperson för		2,0

	kommunikation med IMY. Enligt intervjuade nyckelpersoner har kommunen inget system eller tydligt dokumenterat tillvägagångssätt för hantering av förfrågningar från IMY och registrerade. Enligt *"Hantering av personuppgifter i Svalövs kommun"* ska varje behandling av personuppgifter anmälas till dataskyddsombudet genom att besvara ett webbaserat formulär i ett system. Riktlinjerna behandlar även vilka säkerhetskrav som ska ställas på en personuppgiftsbehandling. Det finns en modul för konsekvensbedömningar i systemet, men kommunen har inget dokumenterat tillvägagångssätt för hur en konsekvensbedömning ska genomföras eller hur säkerhetsåtgärder ska tas fram. En konsekvensbedömning skall göras inför varje ny behandling och exempel på frågor finns listade i riktlinjerna. Dataskyddsombudet kan rådfrågas vid genomförande av konsekvensbedömning. Riktlinjer för gallring av personuppgifter beskrivs i *"Hantering av personuppgifter i Svalövs kommun"*. Respektive nämnd har en egen dokumenthanteringsplan med anvisningar om förvaring och gallring. Överförmyndarnämndens dokumenthanteringsplan uppdaterades senast 2020, övriga nämnders planer uppdaterades senast 2018 eller tidigare. Bortsett från att arkivläggning av diarieförda handlingar ska ske årligen finns det inga dokumenterade anvisningar om hur efterlevnad säkerställs. Enligt intervjuade nyckelpersoner genomförde de år 2018 ett projekt för att kontrollera att gallring verkligen utförs.	Kommunen saknar en dokumenterad rutin för hur förfrågningar från IMY och registrerade ska hanteras. Kommunen saknar en dokumenterad rutin för utförande, och dokumentering, av konsekvensbedömningar. Kommunen genomför ingen kontinuerlig granskning av rutiner och styrdokument kopplat till personuppgiftshanteringen i kommunen.	
Dataskydd	Enligt Svalövs kommuns *"DATASKYDDSPOLICY – interna riktlinjer för hantering av Personuppgifter"* anlitar kommunen endast personuppgiftsbiträden som kan ge garantier för att kraven i dataskyddsförordningen uppfylls. För känsliga personuppgifter ska en snävare behörighetstilldelning tillämpas. Svalövs kommun ska vara beredda att tillmötesgå de rättigheter som registrerade har enligt dataskyddslagstiftningen.		3,0
Utbildning inom dataskydds-förordningen	Enligt Svalövs kommuns *"DATASKYDDSPOLICY – interna riktlinjer för hantering av Personuppgifter"* ska samtliga anställa erbjudas grundläggande dataskyddsutbildning. Enligt informationssäkerhetspolicyn ska anställda regelbundet få information och vid behov erbjudas den utbildning som behövs för att upprätthålla informationssäkerheten. Material ska finnas tillgängligt på intranätet. I december 2020 påbörjades en utbildningsinsats inom GDPR och informationssäkerhet för samtliga anställda. Utbildningen genomförs i form av e-learnings från en extern aktör och består av två obligatoriska kurser		3,0

	inom dataskydd och informationssäkerhet. Fördjupningsutbildningar kommer att erbjudas under andra halvåret 2021. Enligt intervjuade nyckelpersoner kan de med hjälp av det inköpta systemet följa upp och analysera resultatet av utbildningarna. Ca 80% av de anställda ska ha genomfört utbildningen. Enligt intervjuade nyckelpersoner kommer kommunen att lansera en ny utvecklingsplattform under hösten 2021, vilken kommer att erbjuda regelbundna utbildningar och så kallade nano-learnings.		
Molntjänster	Svalövs kommun hanterar personuppgifter i molnet och ska enligt dokumentation underteckna och säkerställa att det finns PUB-avtal i samtliga fall.		3,0

3. Övergripande rekommendationer

Iakttagelser av varierande vikt har identifierats inom olika delar av ramverket. EY har därför valt att presentera de mest relevanta övergripande rekommendationerna för Svalövs kommun och förslag på åtgärder för de främsta riskerna inom informationssäkerhetsarbetet. EY rekommenderar att samtliga förslag åtgärdas inom 12 månader.

Ledningssystem och granskning

EY bedömer att Svalövs kommun saknar viss systematik i sitt arbete med att leda, planera, kontrollera, följa upp och utvärdera den egna verksamhetens arbete med informationssäkerhet. Avsaknad av, eller ett bristfälligt, LIS medför risk för att kommunens informationssäkerhetsarbete bedrivs utan tydliga förhållningspunkter och tillräcklig styrning. EY rekommenderar att kommunstyrelsen tillser att ett LIS utformas i enlighet med kommunens säkerhetsbehov. Kommunen rekommenderas också att implementera en tydlig plan och rutin kring hur arbetet med granskning ska bedrivas inom kommunen. Granskningen bör syfta till att säkerställa att relevanta rutiner efterlevs och att leverantörer agerar i kommunens intresse.

Styrning och rutiner för hantering av personuppgifter

Baserat på genomförd granskning har EY identifierat att vissa av kommunens instruktioner och rutiner för hantering av personuppgifter inte har uppdaterats i tillräckligt hög frekvens. Kommunen saknar dessutom en regelbunden rutin för att granska och säkerställa att hantering av personuppgifter uppfyller kraven i gällande dataskyddsförordning. Det saknas exempelvis en dokumenterad rutin för att följa upp och säkerställa att registerförteckningar och ingångna PUB-avtal är uppdaterade och kompletta över tid. EY rekommenderar således att Svalövs kommun ser över styrdokument och rutiner inom arbetet med hantering av personuppgifter. Kommunen bör säkerställa att relevanta styrdokument existerar samt förblir uppdaterade och aktuella över tid. Slutligen rekommenderar EY att kommunen arbetar vidare med att tillse att existerade rutiner efterlevs i praktiken. Detta genom att kontinuerligt genomföra regelbundna, och planlagda, granskningar och uppföljning.

Styrdokument (policy, strategi och rutiner)

Kommunen har en delvis ostrukturerad hantering och klassificering av dokument relaterat till informationssäkerhet. Informationssäkerhetspolicyn och tillhörande informationssäkerhetsinstruktioner har exempelvis inte uppdaterats sedan 2015. Det saknas också en övergripande riktlinje eller strategi för att leda det kortsiktiga och långsiktiga arbetet med informationssäkerhet. Bristande dokumenthantering och klassificering medför en risk att arbetet med informationssäkerhet fortskrider utan grund i övergripande beslut och utifrån utdaterade metoder, vilket kan leda till att riktighet, spårbarhet, konfidentialitet och tillgänglighet av informationen som hanteras ej säkerställs. EY rekommenderar således att kommunen tillser att styrande dokument uppdateras i enlighet med säkerhetsbehovet eller minst årligen, för att reflektera organisationens nuvarande behov samt omvärldens förändringar och krav. Svalövs kommun rekommenderas dessutom att definiera en tydlig dokumenthierarki som inkluderar versionshistorik, ägarskap, samt omfattning.

4. Revisionsfrågor

Granskningen har utgått från tre revisionsfrågor, vilka besvaras nedan.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Kan styrningen av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?	På en övergripande nivå anses Svalövs kommun arbeta delvis ändamålsenligt med IT- och informationssäkerhet. Under granskningen har Svalövs kommun uppvisat kunskap och ambition inom arbetet med informationssäkerhet. Dock återstår ett antal punkter som behöver adresseras innan EY anser att arbetet kan beskrivas som ändamålsenligt. Kommunen saknar till exempel dokumenterade rutiner inom ett antal områden, exempelvis relaterat till arbetet med personuppgiftsstyrning. Flertalet av de existerande styrdokumenten har dessutom inte uppdaterats med en tillräckligt hög frekvens. Slutligen anser EY att kommunen behöver arbeta vidare med att säkerställa att existerande rutiner och kravställningar efterlevs genom att implementera ett systematiskt arbete med uppföljning och granskning.	
Är arbetet med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?	På en övergripande nivå anses Svalövs kommun inte arbeta ändamålsenligt med att följa upp efterlevnad av beslut och styrdokument relaterat till IT- och informationssäkerhet. I dagsläget saknas en dokumenterad plan för hur arbetet ska bedrivas med att följa upp, och granska, efterlevnaden av kommunens kravställningar och styrdokument inom informationssäkerhet. Viss uppföljning har historiskt sätt genomförts. Avsaknaden av ett strukturerat och kontinuerligt arbete medför dock en risk att informationssäkerhetsarbetet inte bedrivs i	

	enlighet med definierade rutiner och kravställningar.	
Är Svalövs kommuns incidenthanteringsprocess ändamålsenlig?	På en övergripande nivå anses Svalövs kommuns process kring incidentrapportering vara delvis ändamålsenlig. Kommunens incidenthanteringsprocess är standardiserad och utförs med hjälp av systemstöd. Det finns dessutom tydligt definierade roller och ansvar kopplat till processen. Det saknas dock viss spårbarhet i processen, exempelvis relaterat till historiska incidenter och kommunikation kopplat till desamma. EY anser också att kommunen bör granska efterlevnaden av den definierade processen, samt öka medvetenheten kring densamma, innan arbetet kan beskrivas som ändamålsenligt.	

5. Slutsatser

Granskningens syfte har varit 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. Syftet har besvarats med hjälp av följande frågor:

- 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 styrningsdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?
- Är Svalövs kommuns incidenthanteringsprocess ändamålsenlig?

Baserat på den analys och granskning som genomförts bedöms Svalövs kommun i relation till andra offentliga organisationer av liknande storlek och karaktär ha en genomsnittlig mognadsgrad, med ett genomsnitt på 2,41 av 5.00, jämfört med jämförelsetalet 2,27. Detta är dock en lägre mognadsgrad än vad EY rekommenderar för en kommun likt Svalöv, givet den stora mängd information, och andel av känslig karaktär, som hanteras. Mognadsgraden bedöms vara som högst inom nätverk, förändringshantering och utbildning inom dataskyddsförordningen. Lägst anses mognadsgraden vara inom strategi och rutiner, samt personuppgiftsstyrning.

EY rekommenderar att Svalövs kommun förbättrar systematiken i deras informationssäkerhetsarbete, samt dokumenterar tydliga processer och riktlinjer kring hur arbetet med granskning och uppföljning ska genomföras. Detta inkluderar både efterlevnad av styrdokument, samt tredjeparters efterlevnad av på förhand definierade säkerhetskrav. Kommunen bör också säkerställa att arbetet med personuppgiftsstyrning sker på ett ändamålsenligt sätt, vilket inkluderar att ta fram saknade rutiner och att tillse att arbetet sker i enlighet med definierade styrdokument och gällande lagstiftning. Slutligen bör kommunen också säkerställa att styrdokument, och tillhörande riktlinjer, gällande informationssäkerhet förblir riktiga och aktuella över tid.

Stockholm 2021-11-10

Helena Törnqvist, Partner, EY

Bilaga 1: Källförteckning

Intervjuade roller:

- Team lead IT
- Driftchef IT
- Enhetschef Kansli
- Dataskyddsombud
- Trygghets- och säkerhetschef
- IT Chef

Dokumentförteckning:

- BILAGA till kommunstyrelsens rutin för hantering av personuppgiftsincident.pdf
- Dataskyddspolicy 2019.pdf
- Dokumenthanteringsplan BIN.pdf
- Dokumenthanteringsplan BT Kemi 2014-06-18.pdf
- Dokumenthanteringsplan SBN antagen 2018-05-22.pdf
- Dokumenthanteringsplan SN 2012.pdf
- Dokumenthanteringsplan VN.pdf
- Dokumenthanteringsplan ÖF_antagen 200604.pdf
- Dokumenthanteringsplan_KS_antagen 2013-09-09.pdf
- Informations och kommunikationspolicy.pdf
- Informationsplan KS (inte antagen).docx
- Informationssäkerhet sektor vård och omsorg.pdf
- Informationssäkerhetspolicy.pdf
- Molntjänster.docx
- Publiceringsregler webb intra.pdf
- Registerförteckning, Svalövs kommun.xlsx
- Riktlinjer för anmälan av personuppgiftsincidenter enligt datasskyddsförordningen.pdf
- Riktlinjer för hantering av e-post i Svalövs kommun_2doc.docx
- Riktlinjer för hantering av personuppgifter i Svalövs kommun.pdf
- Riktlinjer för tillgänglighet och service, 130917.pdf
- Riktlinjer Sociala medier.pdf
- Rutin för bildningsnämndens hantering av personuppgiftsincidenter.pdf
- Rutin för kommunstyrelsens hantering av personuppgiftsincident.pdf
- Rutin för myndighetsnämndens hantering av personuppgiftsincidenter.pdf
- Rutin för revisionens hantering av personuppgiftsincidenter.pdf
- Rutin för samhällsbyggnadsnämndens hantering av personuppgiftsincidenter.pdf
- Rutin för socialnämndens hantering av personuppgiftsincidenter.pdf
- Rutin för vård- och omsorgsnämndens hantering av personuppgiftsincidenter.pdf
- Rutin för överförmyndarens hantering av personuppgiftsincidenter.pdf
- Rutin utlämnande allmän handling kontra dataskydd.pdf
- Sekretess och känsliga uppgifter i Diabas.pdf
- Utbildning inom dataskyddsområdet.docx
- Svalövs kommun – komplettering.pdf
- Digitaliseringsstrategi för Svalövs kommun.pdf
- Övergripande systematik.pdf
- Svalövs kommun och informationssäkerhet.ppsx
- Behörighetshantering-1.jpg
- Behörighetshantering-2.jpg

- bytlosenord.pdf
- IT-avslut-anvandare.pdf
- 2019 149 Rutin för gallring.pdf
- Bestämmelser om digitalt bevarande av allmänna handlingar i Svalövs kommun.pdf
- RIKTLINJER FÖR ARKIVVÅRD OCH INFORMATIONSFÖRVALTNING-2.pdf
- Rutin för bevarande, gallring och arkivering HSL.pdf

Bilaga 2: Definitioner

Active Directory (AD): Katalogtjänst vilken lagrar information om resurser (såsom användare). Separata IT-system kan kopplas till Active Directory och både inloggning och behörighetsroller i systemen kan således styras genom inställningar och rolluppsättning i Active Directory. Detta möjliggör för central användarhantering och automatisk inloggning.

Applikation: Datorprogram med olika typer av funktionalitet beroende på applikationens syfte. Applikationen finns lagrad på en dator eller en server.

Backup: Säkerhetskopia av den information som finns i en databas eller på en server.

CAB (Change Advisory Board): Styrgrupp för att fatta beslut kring hantering av programförändringar och utveckling av verksamhetens informationssystem.

Databas: En databas är en katalogtjänst med indexerad information om resurser (såsom tex. användare).

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.

E-learning: Utbildning som ges online och/eller via elektroniska hjälpmedel

Förvaltningsobjekt: Styrande enhet inom vilken ett antal olika informationssystem för en viss typ av kommunens verksamhet innefattas. Förvaltningsenheten styrs av en styrgrupp som beslutar om förvaltningsplan och budget. System är uppdelade på olika förvaltningsgrupper inom ett förvaltningsobjekt.

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.

Nano-learning/Nanoutbildning: Korta återkommande utbildningar som erbjuds för anställda.

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

Penetrationstester: Test av informationssystem, nätverk eller webbapplikationer för att identifiera sårbarheter vilka kan utnyttjas av angripare.

Personuppgiftsbiträde: Extern fysisk eller juridisk person som skall säkerställa att personuppgifter hanteras säkert och ändamålsenligt för kommunens räkning.

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.

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

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

Systemförvaltare: Ansvarar för att operativt sköta ett systems förvaltning inom givna ekonomiska ramar.

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.

Systemägare: 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.

Säkerhetskopiering: Kopia av den information som finns i en databas eller på en server.