Revisorerna
SVENLJUNGA KOMMUN

Kommunstyrelsen

AB Svenljunga Bostäder
Svenljunga Verksamhetslokaler AB
Svenljunga Industrifastigheter AB
Svenljunga Kommun Förvaltning AB

För kännedom
Kommunfullmäktige
Samtliga nämnder

**Granskning av IT- och informationssäkerhet**

På uppdrag av revisorerna i Svenljunga kommun och lekmannarevisorerna i de kommunala bolagen har PwC genomfört en granskning av IT- och informationssäkerheten.

Vår samlade bedömning att Svenljunga kommuns IT-säkerhet är tillräcklig för att stödja verksamheten och ge tillräcklig internkontroll. Dock finns det ett antal områden där de inte har en tillräcklig nivå och IT-och informations-säkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll inom IT.

Vi bedömer att Svenljungas kommunala bolags IT-säkerhet inte är tillräcklig för att kunna stödja verksamheten på ett effektivt sätt och ge tillräcklig internkontroll. Under granskningen noterades flera områden där bolagen inte har en tillräcklig nivå avseende IT-och informations-säkerhetsarbetet och som bör förstärkas för att säkerställa en god intern kontroll inom IT.

I bifogad rapport lämnas ett antal rekommendationer vilka vi önskar att kommunstyrelsen och bolagen åtgärdar framöver.

Vi önskar era kommentarer i anledning av utförd granskning senast 2019-06-14.

Svenljunga den 9 april 2019

För valda revisorer

Thomas Mellqvist
Ordförande

Jan-Erik Björkli
Vice ordförande

Bilaga revisionsrapport PwC; *"Granskning av IT- och informationssäkerhet"*

www.pwc.se



# *Granskning av IT- och informationssäkerhet*

## Svenljunga kommun och kommunala bolag

Robin Karlsson
David Hall

Mars 2019

pwc

# *Innehåll*

1. Sammanfattning
2. Inledning
3. Resultat av granskningen
4. Sammanfattande mognadsgrad

*Appendix: Sammanställning avvikelser*

# 1. Sammanfattning

De förtroendevalda revisorerna i Svenljunga kommun har gett PwC i uppdrag att genomföra en granskning av IT-säkerhet för att besvara revisionsfrågan:

*Har kommunstyrelsen och de kommunala bolagen ändamålsenliga policys, rutiner och beskrivningar gällande IT-säkerhet, med fokus på design av rutiner för skydd mot obehörig åtkomst av data och information?*

Efter genomförd granskning är PwCs samlade bedömning att Svenljunga kommuns IT-säkerhet är tillräcklig för att stödja verksamheten och ge tillräcklig intern kontroll. Dock finns det att antal områden där de inte har en tillräcklig nivå och IT- och informationssäkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll inom IT.

PwC bedömer att Svenljungas kommunala bolags (Svenbo) IT-säkerhet inte är tillräcklig för att kunna stödja verksamheten på ett effektivt sätt och ge tillräcklig intern kontroll. Under granskningen noterades flera områden där de inte har en tillräcklig nivå avseende IT- och informationssäkerhetsarbetet och som bör förstärkas för att säkerställa en god intern kontroll inom IT.

Nedan redovisar vi våra mest väsentliga rekommendationer:

- PwC rekommenderar Svenbo att prioritera upplärning av utsedd informationssäkerhetsansvarig för att tillträda rollen snarast. Den som är ansvarig för informationssäkerheten kommer att ha en viktig roll i att definiera, bibehålla samt kommunicera de informationssäkerhetskrav som bolaget har.
- PwC rekommenderar Svenljunga kommun att prioritera revidering av styrande dokumentation för informations- och IT-säkerhet och säkerställa att de regelbundet följs upp och vid behov revideras.
- PwC rekommenderar Svenljunga kommun att färdigställa och Svenbo att påbörja klassificering av IT-system och dokumentera metod i styrande dokumentation. Det är av vikt att ha kännedom om vilka system som är kritiska för verksamheten för att kunna tillämpa nödvändiga skyddsåtgärder.
- PwC rekommenderar Svenljunga kommun och Svenbo att regelbundet genomföra risk- och sårbarhetsanalys för att identifiera väsentliga risker och hot relaterat till IT- och informationssäkerhet.
- PwC rekommenderar Svenljunga kommun och Svenbo att upprätta rutin för hantering av informationssäkerhets-incidenter. Rutinen bör innefatta roller och ansvar, arbetssätt, eskaleringsrutiner och uppföljning av incidenter.
- Svenbo rekommenderas att se över den fysiska säkerheten i serverrummet med avseende på brandsläckningsutrustning, vattenskydd och skydd mot störningar i elförsörjningen av kritiska servrar genom exempelvis UPS-enheter och/eller dieselaggregat.

# 2. Inledning

## 2.1 Bakgrund

Kommunerna blir alltmer beroende av sina system för informationshantering och drift. Ny teknik innebär nya möjligheter men introducerar även nya risker. Kommunikationen med omvärlden ökar i omfattning och systemen blir mer integrerade, såväl inom kommunen som med andra intressenter. Detta ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Den globala hotbilden med risker för intrång förändras kontinuerligt. Informationen måste skyddas mot obehörig åtkomst, såväl externt som internt samtidigt som den skall finnas tillgänglig och dessutom vara tillförlitlig – *rätt information i rätt tid och för rätt personer.*

Mot bakgrund av detta och som ett led i förverkligandet av Svenljunga Kommuns revisionsstrategi har kommunen i sin riskbedömning för 2019 bedömt att en granskning av informations- och IT-säkerheten behöver genomföras för Svenljunga kommun och de kommunala bolagen. De kommunala bolagen benämns härefter för Svenbo.

Granskningen genomförs enligt revisionsplan 2019 som baseras på revisorernas riskbedömning.

## 2.2. Syfte och revisionsfråga

Syftet med granskningen är att besvara revisionsfrågan:

*Har kommunstyrelsen och de kommunala bolagen ändamålsenliga policys, rutiner och beskrivningar gällande IT-säkerhet, med fokus på design av rutiner för skydd mot obehörig åtkomst av data och information?*

## 2.3. Revisionskriterier

Revisionskriterierna för denna granskning har hämtats ur följande:

- Kommunallagen
- Internationella standarder enligt ISO (International Organization for Standardization) avseende Informationsteknik, Säkerhetstekniker och Ledningssystem för informationssäkerhet (ISO 27001:2013)
- Internationella standarder enligt COBIT (Control Objective for Information and Related Technology Standards) avseende informationssäkerhet.

# 2. Inledning

## 2.4 Kontrollmål

Kontrollmålen och bedömningen av dessa möjliggör att revisionsfrågan kan besvaras. Följande kontrollmål har bedömts som viktiga för granskningen:

1. Finns det en adekvat övergripande styrning av informations- och IT-säkerheten?
2. Finns det styrande dokument, såsom policy och riktlinjer för informations- och IT-säkerhet, och täcker detta in samtliga informations- och driftsystem samt underliggande infrastruktur?
3. Finns formellt beskrivna rutiner för att identifiera och hanteras nya risker och hot?
4. Finns formellt beskrivna rutiner för att upptäcka och hantera icke önskvärda incidenter både internt och externt på ett ändamålsenligt sätt?
5. Finns formellt beskrivna rutiner framtagna för hantering av tilldelning och övervakning av behörigheter, både kommunens användare men även konsulters aktiviteter i systemen?
6. Finns formellt beskrivna rutiner framtagna för att hantera ändring av systemens informationsbearbetning (exempelvis ändringar av rapporter och automatiska flöden)?
7. Finns formellt beskrivna rutiner framtagna för fysiskt och logiskt skydd av data och information (exempelvis lösenordsskydd och inpasseringsskydd)?
8. Finns formellt beskrivna rutiner för hantering av outsourcing till externa leverantörer, exempelvis former för kravställande och kommunikation, avtal och uppdatering av dessa, samt uppföljning av efterlevnad avtal?
9. Finns rutiner för att säkerställa att nämnders styrande dokument adresserar områden kring IT- och informationssäkerhet där ej kommunstyrelsens styrande dokument är applicerbara?

## 2.5 Metod och avgränsningar

Granskningen har utförts enligt god revisionssed med utgångspunkt i "Vägledning för verksamhetsrevision i kommuner och landsting" från Sveriges kommunala yrkesrevisorer (SKYREV). Granskningen av processer inom IT-säkerhet utfördes genom intervjuer med berörda personer samt granskning av relevant dokumentation.

Följande personer har varit intervjuade i granskningen:

Svenljunga kommun:
- Christian Bonfré (Digitaliseringschef)
- Magnus Nilsson (Kommunchef)
- Fredrik Ekberg (Samhällsbyggnadschef)
- Tommy Fock (Barn & Utbildningschef)
- Johan Skön (IT-strateg, Barn & Utbildning)
- Kristin Johansson (Administratör, Barn & Utbildning)
- Liselott Johansson (Nämndsekreterare, Socialförvaltningen)
- Monica Dahlgren Svensson (Systemförvaltare, Socialförvaltning)

Kommunala bolag (Svenbo):
- Henrik Öst (VD)
- Johnny Verkander (Fastighetsförvaltare)

Granskningen har genomförts under mars 2019 av Robin Karlsson (projektledare) och David Hall, båda från PwC. Rapporten har kvalitetssäkrats av Ragnar Bergvik på PwC.

# 3. Resultat av granskningen

## 3.1 Finns det en adekvat övergripande styrning av informations- och IT-säkerheten?

### *Iakttagelser*

Svenljunga kommun har en IT-avdelning bestående av åtta personer. IT-avdelningen leds av en Digitaliseringschef som bland annat ansvarar för IT-drift och informationssäkerhet. Kommunens IT-avdelning arbetar med drift av kommunens IT-miljö och är inte involverade i de kommunala bolagens arbete gällande IT- och informationssäkerhet. Kommunen har även systemförvaltare och systemansvariga i varje enskild förvaltning där utpekade roller finns för delar av arbetet med informations- och IT-säkerhet. Exempelvis för att hantera behörigheter till förvaltningsspecifika system.

Svenbo har ingen IT-avdelning utan driften av IT-miljön är outsourcad till extern leverantör. De har ingen IT-chef eller informationssäkerhetsansvarig utan det är i nuläget VD som ansvarar för informations- och IT-säkerhetsarbetet. En person har däremot blivit utsedd till att bli ansvarig för informationssäkerhetsarbetet, men tjänsten var under genomförandet av granskningen inte tillträdd.

Gemensam iakttagelse för både Svenljunga kommun och Svenbo är att både har påbörjat ett arbete med att upprätta personuppgiftsavtal med relevanta parter men arbetet är inte slutfört.

### *Bedömning*

Vår bedömning är att Svenljunga kommun har en tillräcklig nivå gällande styrning av informations- och IT-säkerhet. Detta då kommunens organisation har tydliga funktioner för IT- och informationssäkerhet. Vid granskningen noterades inga iakttagelser som bedöms som hög risk för kontrollmålet.

Gällande Svenbo är vår bedömning att Svenbo saknar en tillräcklig nivå gällande styrning av informations- och IT-säkerhet. Detta främst då Svenbo saknar en dedikerad informationssäkerhetsansvarig i nuläget.

PwC rekommenderar Svenbo att prioritera upplärning av utsedd informationssäkerhetssamordnare för att tillträda rollen snarast.

PwC rekommenderar Svenljunga kommun och Svenbo att färdigställa upprättandet av personuppgiftsbiträdesavtal med nödvändiga parter.

Se område 3.1 i appendix för mer information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.2 Finns det styrande dokument, såsom policy och riktlinjer för informations- och IT-säkerhet och täcker detta in samtliga informations- och driftsystem samt underliggande infrastruktur?

### Iakttagelser

Svenljunga kommun och Svenbo har båda flera styrande dokument gällande IT. Bland annat har de en IT-policy, informationssäkerhetspolicy samt instruktioner som beskriver regler och ansvar för alla användare av IT-miljön. Vid granskning av dokumentation noterades att flera dokument inte reviderats på över 10 år. Det finns en uppdaterad informationssäkerhetspolicy som vid granskningstillfället var under godkännandeprocess, samt pågår det ett arbete med att uppdatera underläggande styrdokument.

Vid samtal med personal inom Svenljunga kommuns förvaltningar framkom det även att personal inte var medveten om att de var ansvariga för att följa upp och revidera deras förvaltningsspecifika dokumentation.

Svenbo har nyligen tagit fram policys och instruktioner för IT- och informationssäkerhet, inklusive IT-policy och informationssäkerhetspolicy. Tidigare saknades det styrande dokumentation för detta område.

En gemensam iakttagelse för Svenljunga kommun och Svenbo är att båda parterna saknar ett implementerat internt kontrollramverk gällande IT.

### Bedömning

Vår bedömning är att Svenljunga kommun och Svenbo i nuläget har en tillräcklig nivå gällande styrande dokument då båda parterna har styrande dokument som täcker in samtliga informations- och driftsystem. PwC noterade däremot ett antal förbättringsmöjligheter för båda parter. Följande rekommendationer lämnas mot bakgrund till iakttagelserna:

PwC rekommenderar Svenljunga kommun att prioritera revidering av styrande dokumentation för informations- och IT-säkerhet och säkerställa att de regelbundet följs upp och vid behov revideras.

PwC rekommenderar Svenljunga kommun och Svenbo att implementera ett internt kontrollramverk över relevanta kontroller som utförs i organisationerna kopplat till IT.

Se område 3.2 i appendix för mer information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.3 Finns formellt beskrivna rutiner för att identifiera och hanteras nya risker och hot?

### Iakttagelser

Svenljunga kommun arbetar med att genomföra riskanalyser av IT-system i verktyget KLASSA som används för att klassificera system. Vid granskningstillfället var dessa analyser påbörjade men inte färdigställda.

Svenljunga kommun saknar kontinuitetsplan och avbrottsplan. En kontinuitetsplan är ett företagsövergripande dokument som används för att säkerställa att verksamheten har effektiva processer, system och stöd för att motverka avbrott i verksamheten. Gällande avbrottsplanering har Svenljunga kommun en dokumenterad prioriteringslista, för hur IT-enheten ska arbeta med att prioritera återställning av system om samtliga IT-system och infrastruktur slagits ut. Vidare har Svenljunga kommun inte genomfört någon övergripande risk- och sårbarhetsanalys avseende informations- och IT-säkerhet.

Svenbo har inte arbetat med att klassificera IT-system, inte tagit fram kontinuitetsplan eller avbrottsplaner, samt inte genomfört någon risk- och sårbarhetsanalys. Svenbo har i sin nya IT-policy fastslagit att en risk- och sårbarhetsanalys ska genomföras varje år men då IT-policyn skapades i början av 2019 har ingen risk- och sårbarhetsanalys genomförts vid granskningstillfället.

Det noterades även att framtagandet av en kontinuitetsplan är outsourcat till en extern konsultfirma och att man vid granskningstillfället hade kommit ungefär halvvägs.

### Bedömning

Vår bedömning är att Svenljunga kommun och Svenbo i nuläget ej har en tillräcklig nivå gällande rutiner för att identifiera och hantera risker och hot då formella riskanalyser för IT- och informationsrisker ej genomförts samt att färdigställda kontinuitetsplaner och avbrottsplaner saknas.

PwC rekommenderar Svenljunga kommun att färdigställa och Svenbo att påbörja klassificering av IT-system och dokumentera metod i styrande dokumentation. Det är av vikt att ha kännedom om vilka system som är kritiska för verksamheten.

PwC rekommenderar Svenljunga kommun och Svenbo att regelbundet genomföra risk- och sårbarhetsanalys för att identifiera väsentliga risker och hot relaterat till IT- och informationssäkerhet.

PwC rekommenderar Svenljunga kommun och Svenbo att utveckla övergripande kontinuitetsplan för att säkerställa att verksamheten har effektiva processer, system och stöd för att motverka långvariga avbrott i verksamheten. Kontinuitetsplan kan ses som kravställare till IT-avdelningen vid utformning av avbrottsplan.

PwC rekommenderar att Svenljunga kommun och Svenbo utvecklar avbrottsplan, innefattande hur allvarliga avbrotts-situationer ska hanteras och nödvändiga åtgärder för att få tillbaka IT-stödet enligt verksamhetens krav, samt testa planen regelbundet.

Se område 3.3 i appendix för mer information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.4 Finns formellt beskrivna rutiner för att upptäcka och hantera icke önskvärda incidenter både internt och externt på ett ändamålsenligt sätt?

### Iakttagelser

Svenljunga kommun saknar en formell rutinbeskrivning för incidenthantering. Enligt intervju framgår däremot att IT-enheten har ett välfungerande arbetssätt avseende rapportering och hantering av incidenter.

Kommunen har beskrivning i styrande dokumentation för hur incidenter ska rapporteras samt att IT-chefen ansvarar för uppföljning och rapportering till kommunledningsgruppen. Inom IT-enheten finns även en mall för att beskriva inträffade incidenter, hantering av dem och förbättringsåtgärder, vilket används som underlag vid uppföljning av incidenter.

Även Svenbo saknar styrande dokumentation för att hantera incidenter. I nuläget ska alla ärenden rapporteras till VD, vilket beskrivs i styrande dokumentation.

Under granskningen noterades att en förvaltning i Svenljunga kommuner har rutiner för att följa upp loggar av användaraktiviteter i ett kritiskt system. I övrigt noterades inga ytterligare system inom kommunen eller Svenbo där uppföljning av loggar sker.

Svenljunga kommun genomför regelbundet återläsningstester av säkerhetskopior. Svenbo har inga rutiner för återläsningstester av säkerhetskopior. Både Svenljunga kommun och Svenbo har flera säkerhetskopior förvarade på olika platser för att säkerställa redundans.

### Bedömning

Vår bedömning är att Svenljunga kommun och Svenbo inte har en tillräcklig nivå gällande incidenthantering då de saknar rutiner för att hantera informationssäkerhets-incidenter.

PwC rekommenderar Svenljunga kommun och Svenbo att upprätta styrande dokumentation för hur informationssäkerhetsincidenter ska hanteras inom organisationen. Rutin bör innefatta roller och ansvar, arbetssätt, eskaleringsrutiner och uppföljning av incidenter.

PwC rekommenderar Svenljunga kommun och Svenbo att utreda om det finns behov och möjlighet att logga och följa upp användares kritiska aktiviteter som utförs av konton med höga behörigheter. Utred även behovet av att införa system som hjälper till att filtrera loggar för att underlätta granskning av dem. Systemet bör utifrån loggarna indikera vissa förutbestämda mönster som kan tyda på en eventuell attack.

PwC rekommenderar Svenbo att regelbundet testa återläsning av säkerhetskopior och dokumentera resultat.

Se område 3.4 i appendix för mer information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.5 Finns formellt beskrivna rutiner framtagna för hantering av tilldelning och övervakning av behörigheter, både kommunens användare men även konsulters aktiviteter i systemen?

### Iakttagelser

Svenljunga kommun har en dokumenterad rutin (IT-säkerhetsinstruktion: Förvaltning) för beställning av åtkomst till IT-system. Dokument är däremot inte reviderat sedan 2007-02-06 och därtill står det i fastställt dokument att arbetssättet är "under framtagning för kvalitetssäkring". Vissa förvaltningar har upprättat egna rutinbeskrivningar för delar av hantering av behörigheter. Svenljunga har automatiserat processen för exempelvis tilldelning och borttag av behörigheter i AD. Under granskningen noterades att kommunen har externa leverantörer som har tillgång till opersonliga systemkonton, vilket försämrar spårbarheten av konsultens aktiviteter.

Svenbo har nyligen framtagna rutiner för behörighetstilldelning till nyanställda och hur borttagning av behörigheter sker i verksamhetens system. Däremot saknas rutin för hur förändring av befintliga anställdas behörigheter skall ske, om de t.ex. skulle byta position inom organisationen och behöver utökade/minskade/ändrade behörigheter. Vidare noterade PwC att Svenbos lösenordspolicy endast kräver ett 6 tecken långt lösenord vilket är kortare än vad PwC anser är good practice.

En gemensam iakttagelse för Svenljunga kommun och Svenbo är att det saknas en rutin för regelbunden genomgång av användares behörigheter, för att säkerställa att endast godkända användare har behörighet och att användare har korrekt behörighet. Svenljunga kommun har en process för att konton per automatik ska tas bort när anställda avslutar sin anställning.

### Bedömning

Vår bedömning är att Svenljunga kommun och Svenbo inte har tillräcklig nivå gällande om det finns formellt beskrivna rutiner för hantering av tilldelning och övervakning av behörigheter. Svenljunga kommun har automatiserat delar av behörighetshanteringen men saknar dokumenterade rutiner. Svenbo har rutiner för tilldelning av behörigheter för nyanställda och borttag av behörigheter för personer som slutar.

PwC rekommenderar Svenljunga kommun att se över och uppdatera rutin för hantering av behörigheter där det behövs så att den speglar dagens arbetssätt, samt beskriva arbetssätt för förändring och borttag av behörigheter.

PwC rekommenderar Svenbo att uppdatera sina behörighetsrutiner till att även inkludera förändring av befintliga behörigheter.

PwC rekommenderar Svenljunga kommun att se över skapandet av externa leverantörers användarkonton då det framkom att leverantörer har tillgång till systemkonton, då de endast ska ha personliga konton.

PwC rekommenderar Svenbo att uppdatera sin lösenordspolicy gällande kravet på antal tecken till minst 8 tecken.

PwC rekommenderar både Svenljunga kommun och Svenbo att skapa en formell rutin för att regelbundet granska behörigheter med syftet att säkerställa att endast godkända användare har behörighet, samt att dessa användare har korrekt behörighet i applikationer och infrastruktur (operativsystem, servrar och databaser).
Se område 3.5 i appendix för mer information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.6 Finns formellt beskrivna rutiner framtagna för att hantera ändring av systemens informationsbearbetning (exempelvis ändringar av rapporter och automatiska flöden)?

### Iakttagelser

Svenljunga kommun har formella processbeskrivningar för hur programförändringar genomföras. Majoriteten av system är outsourcade och driftas inte av kommunen. Leverantörerna som driftar systemen behöver tillåtelse från Svenljunga kommuns IT-avdelning varje gång de behöver tillgång till systemen och som regel ska personliga användarkonton användas. Under granskningen noterades det dock att det finns externa leverantörer som har tillgång till systemkonton (se ytterligare under avsnitt 3.5 ).

PwC noterade att Svenbo har ett dokument för förändring och hantering av uppdatering av IT-system, som beskriver om uppdatering sker per automatik eller manuellt, samt att VD beslutar om genomförande av alla manuella uppdateringar. Dokument är kortfattat och saknar flera relevanta områden som bör finnas i en rutin för förändringshantering.

### Bedömning

PwC bedömer att Svenljunga kommun har en tillräcklig nivå gällande hantering av programförändringar. Detta då rutiner för hantering av programförändringar finns på plats.

Vår bedömning gällande Svenbo är att de inte har en tillräcklig nivå gällande hantering av programförändringar då det saknas relevant styrande dokumentation.

Följande rekommendation lämnas mot bakgrund till iakttagelserna:

PwC rekommenderar Svenbo att införa en formell rutin för förändringshantering och kommunicera denna med berörda leverantörer. Rutinen bör hantera alla typer av förändringar dvs. normala och akuta för både mjuk- och hårdvara.

Se område 3.6 i appendix för mer detaljerad information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.7 Finns formellt beskrivna rutiner framtagna för fysiskt och logiskt skydd av data och information (exempelvis lösenordsskydd och inpasseringsskydd)?

### Iakttagelser

Svenljunga kommun och Svenbo har inbrottslarm till kontors- och datorutrymmen samt avtal med vaktbolag vid larm.

Svenljunga kommun har ett datacenter på plats i kommunhuset för driften av kommunens IT- och systemmiljö. Datacentret har inpasseringsskydd, temperatur- och fuktövervakning och skydd mot bortfall i elförsäljning (UPS och dieselaggregat). Användande av de nyckelkort som behövs för att få tillträde till datacentret loggas men ingen uppföljning av tillträden görs.

Svenbo har sitt serverrum i samma byggnad som kontorslokalerna. Serverrummet saknar brandlarm, kylaggregat, vattenskydd och skydd mot bortfall i elförsörjning.

För iakttagelser gällande logiskt skydd av data och information se avsnitt 3.5.

### Bedömning

Vår bedömning är att Svenljunga kommunen har en tillräcklig nivå gällande fysisk säkerhet och logiskt skydd då tillträdesskydd finns till lokaler och det finns en rimlig nivå av skydd mot brand, fukt, värme etc. Vid granskningen noterades inga iakttagelser som bedöms som hög eller medium risk.

Gällande Svenbo är vår bedömning att det inte finns en tillräcklig nivå gällande fysisk säkerhet och logiskt skydd av information. Detta baseras på avsaknaden av ett brandlarm, kylaggregat, vattenskydd, UPS och dieselaggregat kopplat till datorutrymmen.

PwC rekommenderar Svenbo att se över den fysiska säkerheten i serverrummet med avseende på brandsläckningsutrustning, vattenskydd och skydd mot störningar i elförsörjningen av kritiska servrar genom exempelvis UPS-enheter och/eller diesel aggregat.

Se område 3.7 i appendix för mer information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.8 Finns formellt beskrivna rutiner för hantering av outsourcing till externa leverantörer, exempelvis former för kravställande och kommunikation, avtal och uppdatering av dessa, samt uppföljning av efterlevnad avtal?

### Iakttagelser

I Svenljunga kommun är det systemförvaltare som driver upphandlingar av IT-tjänster och tar stöd av andra personer i kommunen såsom digitaliseringschefen. Man litar på att krav som ställs i upphandlingen följs och ingen uppföljning av leverantörens avtalade mål sker.

Hos Svenbo är det VDn som genomför upphandlingar av IT-lösningar och de har en leverantör för driften av deras IT-miljö.

Svenbo har en utsedd kontaktperson hos leverantör som hjälper Svenbo och VDn med majoriteten av alla IT-frågor som uppstår. Avtalet med leverantör är ett rullande kontrakt på 1 år.

### Bedömning

Vår bedömning är att Svenljunga kommun och Svenbo har en tillräcklig nivå gällande outsourcing och upphandlingar kopplat till IT. Vid granskningen noterades inga iakttagelser som bedöms som hög risk.

PwC rekommenderar Svenljunga kommun och Svenbo att ställa tydliga krav gentemot leverantören på förväntad leverans inom olika områden gällande drift, avbrottsplanerings och infrastruktur. Uppfyllande av krav ska även kunna bekräftas från leverantörens sida, exempelvis i rapportform.

Se område 3.8 i appendix för mer information om iakttagelser och rekommendationer.

# 3. Resultat av granskningen

## 3.9 Finns rutiner för att säkerställa att nämnders styrande dokument adresserar områden kring IT- och informationssäkerhet där ej kommunstyrelsens styrande dokument är applicerbara?

### *Iakttagelser*

Svenljunga kommun har flertalet styrande dokument avseende informations- och IT-säkerhet, som är kommunövergripande. Vid samtal med personal inom kommunala förvaltningar framkom att de är medvetna och utgår från kommunövergripande styrande dokument vid utformning av förvaltningsspecifik dokumentation.

Det finns däremot inte någon styrande dokumentation som säkerställer att nämnders styrande dokument adresserar områden kring IT- och informationssäkerhet.

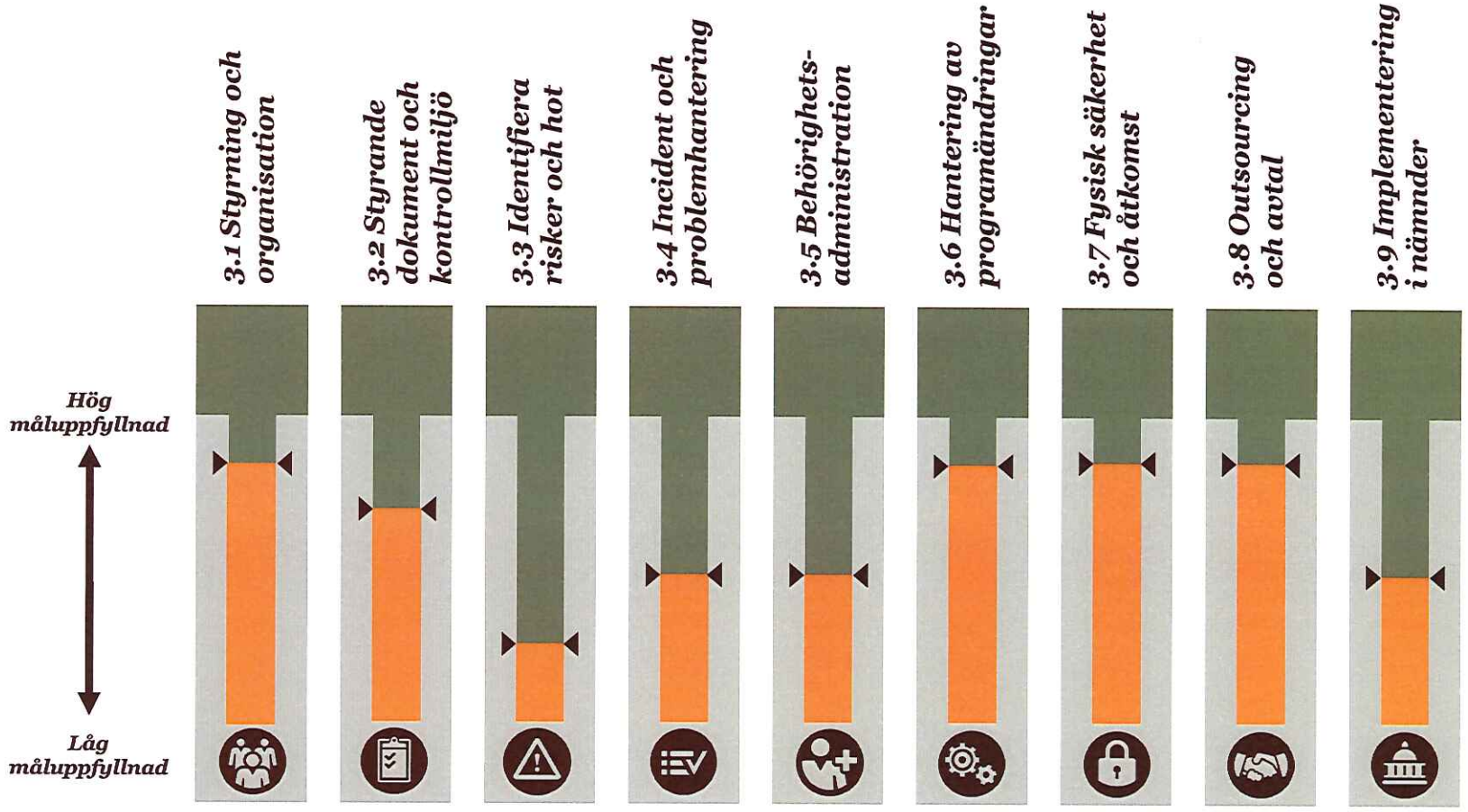
### *Bedömning*

Vår bedömning är att Svenljunga kommun inte har rutiner för att säkerställa att nämnders styrande dokument adresserar områden kring IT- och informationssäkerhet där ej kommunstyrelsens styrande dokument är applicerbara. Detta då det inte specificeras i kommunens övergripande dokument att nämnderna måste utgå från dessa vid framtagande av sina egna styrande dokument.

PwC rekommenderar Svenljunga kommun att upprätta rutiner i styrande dokument för att säkerställa att nämndspecifika styrande dokument adresserar områden kring informations- och IT-säkerhet.

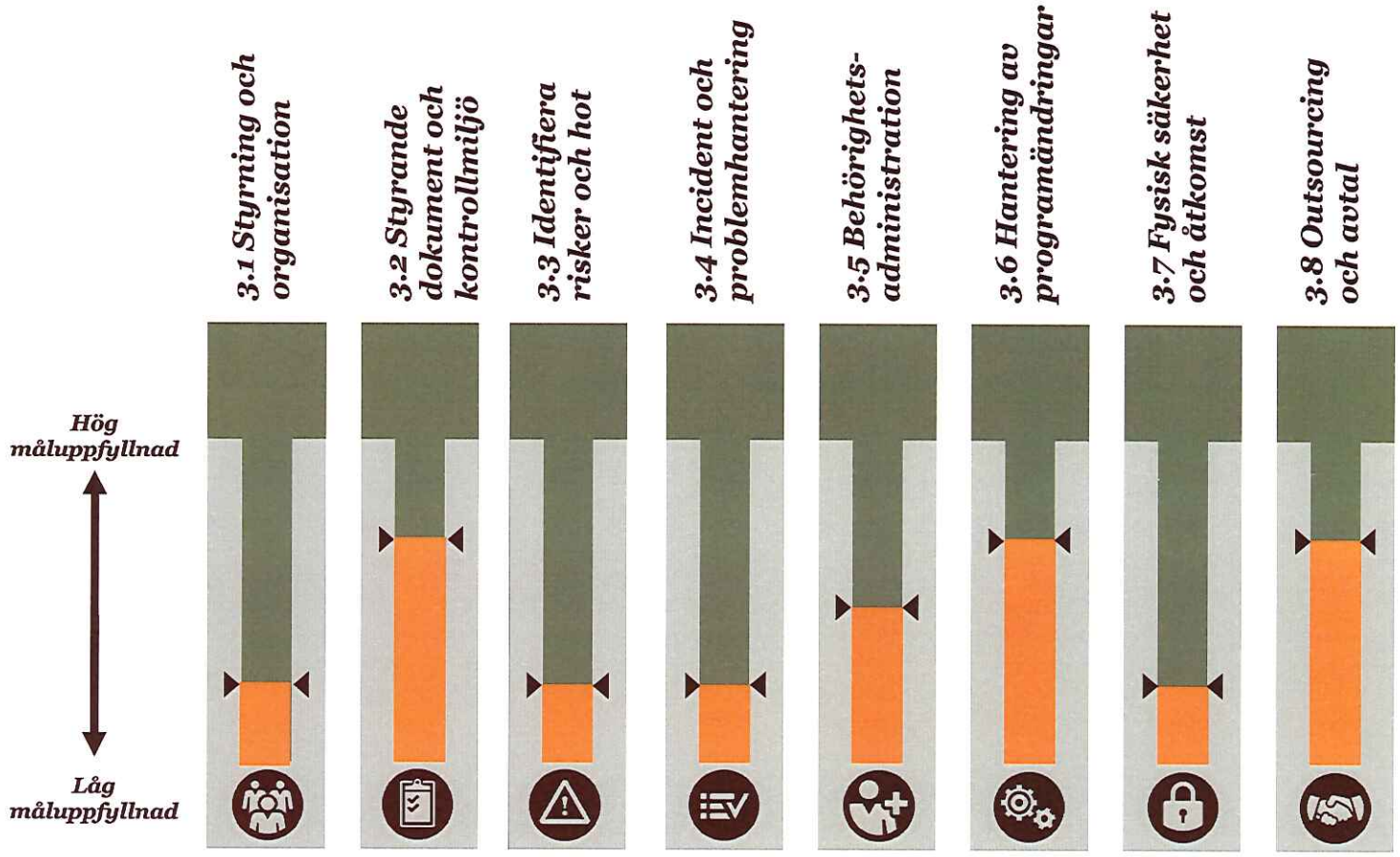
# 4.1 Svenljunga kommun
## Sammanfattande mognadsgrad per kontrollmål

Nedan redovisas en sammanfattande illustrativ översikt för mognadsgrad per granskningsområde. Mognadsgrad baseras på antal avvikelser och riskbedömning av desamma inom respektive kontrollmål.



# 4.2 Svenbo
## Sammanfattande mognadsgrad per kontrollmål

Nedan redovisas en sammanfattande illustrativ översikt för mognadsgrad per granskningsområde. Mognadsgrad baseras på antal avvikelser och riskbedömning av desamma inom respektive kontrollmål.



**Datum:**

**Robin Karlsson**
*Projektledare*

**Fredrik Carlsson**
*Uppdragsledare*

**David Hall**
*Projektmedlem*

# *Appendix: Sammanställning avvikelser*

På följande sidor redogör vi mer i detalj för de avvikelser och risker som vi har sett i vår granskning, kopplat till respektive kontrollmål. Vi ger även rekommendationer för noterade avvikelser.

Vi har gjort en prioritering av avvikelserna där L står för låg prioritet, M för medel och H för hög. Definitionen av denna klassificering visas nedan:

| Prioritet | Förklaring till prioritet |
|---|---|
| Hög | Syftar på en svaghet som har stor inverkan på system, processer och relaterade kontroller och som kan utsätta enheten för större förluster, ineffektivitet och/eller kan resultera i en väsentlig felaktighet i räkenskaperna. |
| Medel | Syftar på en situation eller arbetssätt som skiljer sig från vad PwC anser vara god praxis och som vi bedömer har en negativ inverkan på den interna kontrollen. |
| Låg | Syftar på en situation eller arbetssätt som enbart har en begränsad effekt på den interna kontrollen. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.1 | H | Vid granskningen noterades det att Svenbo i nuläget saknar en informationssäkerhetsansvarig. | För att kunna skapa och bibehålla tillräcklig kontroll över bolagets information och säkerställa välgrundade prioriteringar är det viktigt att utse en roll med ett formellt övergripande informationssäkerhetsansvar. | PwC rekommenderar Svenbo att prioritera upplärning av utsedd informationssäkerhetsansvarig för att tillträda rollen snarast. Den som är ansvarig för informationssäkerheten kommer att ha en viktig roll i att definiera, bibehålla samt kommunicera de informationssäkerhetskrav som bolaget har. |
| 3.1 | M | Svenljunga kommun och Svenbo arbetar med att upprätta personuppgiftsbiträdesavtal med relevanta parter. Detta arbetet är inte klart och alla nödvändiga avtal är inte upprättade. | Utan tydlig ansvarsfördelning avseende hantering av personuppgifter ökar risken för att personuppgifter inte hanteras ändamålsenligt och att GDPR inte efterlevs. | PwC rekommenderar att Svenljunga kommun och Svenbo upprättar personuppgiftsbiträdesavtal med alla nödvändiga parter. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.2 | H | PwC noterade att Svenljunga kommun har styrande dokument avseende IT- och informationssäkerhet som inte reviderats på över 10 år.<br><br>I nuläget pågår arbetet med att godkänna en ny informationssäkerhetspolicy, samt att underliggande styrdokument uppdateras. | När dokument inte regelbundet följs upp och uppdateras riskerar dem att bli inaktuella. Då ökar risken för att de inte är i linje med den IT- och informationssäkerhet som organisationerna behöver. | PwC rekommenderar Svenljunga kommun att prioritera revidering av styrande dokumentation för informations- och IT-säkerhet och säkerställa att de regelbundet följs upp och vid behov revideras. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.2 | M | Svenljunga kommun och Svenbo saknar ett ramverk för intern kontroll gällande IT. | Vid avsaknad av kontrollramverk ökar risken för att kvalitet, nivå av spårbarhet och utförande av kontroll blir personberoende. | PwC rekommenderar Svenljunga kommun och Svenbo att arbeta fram och implementera ett kontrollramverk för relevanta kontroller som utförs i organisationen kopplat till IT. Följande bör ingå i kontroll-ramverket:<br>• Vilken risk hanteras genom kontrollen<br>• På vilket sätt kontrollen skall utföras (kontrollaktivitet och design).<br>• Varför ska kontrollen utförs (mål och syfte).<br>• Vem som skall utföra kontrollen<br>• Hur ofta skall kontrollen utföras.<br>• Vilken dokumentation skall sparas för att verifiera genomförd kontroll (bevis för spårbarhet).<br>• Vad skall göras om en kontroll uteblir eller är ineffektiv (Åtgärd). |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.3 | H | PwC noterade vid granskningen att Svenljunga kommuns arbete med att klassificera IT-system inte är slutfört. Svenbo har ej påbörjat klassificering av IT-system. | Vid avsaknad av klassificering av system riskerar kommunerna att inte veta vilka system som är kritiska för verksamheten samt vilka skyddsåtgärder som är nödvändiga för att exempelvis minimera risk för avbrott i system och lämpligt skydd mot obehörig åtkomst. | PwC rekommenderar Svenljunga kommun att färdigställa och Svenbo att påbörja klassificering av IT-system och dokumentera metod i styrande dokumentation. Det är av vikt att ha kännedom om vilka system som är kritiska för verksamheten för att kunna tillämpa nödvändiga skyddsåtgärder. |
| 3.3 | M | Svenljunga kommun eller Svenbo har inte genomfört risk- och sårbarhetsanalyser. Svenbo upprättade nyligen en ny IT-policy som specificerar att en risk- och sårbarhetsanalys skall genomföras varje år. Svenljunga kommun har påbörjat klassificering av IT-system som ger bra underlag till arbetet med risk- och sårbarhetsanalys. | Om organisationen ej kontinuerligt genomför risk- och sårbarhetsanalyser riskerar dem att missa nyuppkomna hot eller interna sårbarheter för verksamheten. | PwC rekommenderar Svenljunga kommun och Svenbo att regelbundet genomföra risk- och sårbarhetsanalys för att identifiera väsentliga risker och hot relaterat till IT- och informationssäkerhet.<br><br>Resultatet kan utgöra underlag för framtagande av kontinuitetsplan. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.3 | M | Vid granskningen noterades att varken Svenljunga kommun eller Svenbo har en kontinuitetsplan. | Avsaknad av dokumenterade kontinuitetsplaner medför som regel att en katastrof eller ett längre avbrott får allvarligare konsekvenser än vad som skulle ha varit fallet om en existerande och testad plan funnits. Brister i katastrof- och kontinuitetsplanering leder även till en ökad risk för att verksamheten blir utan systemstöd längre än nödvändigt samt att verksamheten avstannar helt vid systembortfall. | PwC rekommenderar Svenljunga kommun och Svenbo att utveckla övergripande kontinuitetsplan för att säkerställa att verksamheten har effektiva processer, system och stöd för att motverka långvariga avbrott i verksamheten. Kontinuitetsplan kan ses som kravställare till IT-avdelningen vid utformning av avbrottsplan. |
| 3.3 | M | Vid granskningstillfället noterades det att Svenljunga kommun och Svenbo inte har en komplett och uppdaterad avbrottsplan. | Avsaknad av dokumenterad avbrottsplan medför som regel att en katastrof eller ett längre avbrott får allvarligare konsekvenser än vad som skulle ha varit fallet om en existerande och testad plan funnits. | PwC rekommenderar att Svenljunga kommun och Svenbo utvecklar avbrottsplan som innefattar hur allvarliga avbrottssituationer ska hanteras och nödvändiga åtgärder för att få tillbaka IT-stödet enligt verksamhetens krav, samt testa planen regelbundet. Test av plan innefattar återläsning av säkerhetskopior. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.4 | H | Under granskningen noterades det att Svenbo och Svenljunga kommun saknar en rutiner för hur incidenter och problem skall hanteras inom organisationen. Svenbo saknar även rutiner för uppföljning av incidenter. | Inträffade incidenter bör identifieras, rapporteras och hanteras så snart som möjligt för att minimera risken för att verksamheten skadas samt undvika kostsamma åtgärder.<br><br>Utan uppföljning av incidenter finns ökad risk för att grundorsaker till en grupp av incidenter inte identifieras och resurser för att lösa återkommande incidenter felprioriteras | PwC rekommenderar Svenljunga kommun och Svenbo att upprätta rutin för hantering av informationssäkerhetsincidenter. Rutinen bör innefatta roller och ansvar, arbetssätt, eskaleringsrutiner och uppföljning av incidenter. |
| 3.4 | L | PwC noterade under granskningen att Svenljunga kommun och Svenbo inte analyserar loggar för aktiviteter i kritiska system av användare med höga behörigheter. | Utan loggning av användares aktiviteter kan det medföra att felaktigheter och obehörig åtkomst inte upptäcks i tid, alternativt inte upptäcks alls. | PwC rekommenderar Svenljunga kommun och Svenbo att utreda om det finns behov och möjlighet att logga och följa upp användares kritiska aktiviteter som utförs av konton med höga behörigheter. Utred även behovet av att införa system som hjälper till att filtrera loggar för att underlätta granskning av dem. Systemet bör utifrån loggarna indikera vissa förutbestämda mönster som kan tyda på en eventuell attack. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.4 | M | Under granskningen blev vi informerade om att Svenbo inte har någon rutin för att regelbundet testa återläsning av säkerhetskopior. | Om man inte regelbundet testar att återläsning från säkerhetskopiorna fungerar på ett tillfredställande sätt finns risk att de inte fungerar när det behövs, t ex vid en katastrofsituation.<br><br>Utan fungerande säkerhetskopior från systemen kan återstarttiden för verksamheten bli orimligt lång vilket kan få konsekvenser för verksamheten. | PwC rekommenderar Svenbo att regelbundet testa återläsning av säkerhetskopior och dokumentera resultat. |

# Sammanställning avvikelser

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.5 | M | Svenljunga har en beskrivning för tilldelning av behörigheter i styrande dokument. Dokument har inte reviderats sedan 2007 och rutinbeskrivning bör ses över för att överensstämma med dagens arbetssätt, samt lägga till beskrivning för förändring och borttag av behörighet. | Att inte ha en uppdaterad och komplett rutin för hantering av behörigheter kan medföra att behörigheter tilldelas till personal som inte ska ha tillgång till en specifik resurs eller tjänst. Det kan även innebära att eventuella förändringar av behörigheter blir felaktiga samt att behörigheter som ska tas bort ligger kvar onödigt länge. Detta kan äventyra säkerheten för Svenljunga kommuns IT-system och information. | PwC rekommenderar Svenljunga kommun att se över och uppdatera rutin för hantering av behörigheter där det behövs så att den speglar dagens arbetssätt, samt beskriva arbetssätt för förändring och borttag av behörigheter. Rutinen bör bygga på att en formell ansökan om behörighet skickas till IT-avdelningen. Ansökan bör vara undertecknad av närmaste chef och/eller systemägare för den som skall ha behörighet. Detta bör även gälla vid förändring och borttagande av behörigheter. |
| 3.5 | M | PwC noterade att Svenbo har formella processer för tilldelning av behörigheter för nyanställda och borttag av behörigheter för personer som slutar. Däremot saknas en rutinbeskrivning för hur förändring av redan befintliga behörigheter skall gå till. | Att inte ha en uppdaterad och komplett rutin för hantering av behörigheter kan medföra att behörigheter tilldelas till personal som inte skall ha tillgång till en specifik resurs eller tjänst. Det kan även innebära att eventuella förändringar av behörigheter blir felaktiga samt att behörigheter som skall tas bort ligger kvar onödigt länge. Detta kan äventyra säkerheten för Svenljunga kommuns IT-system och information. | PwC rekommenderar Svenbo att skapa en formell rutinbeskrivning avseende förändring av redan befintliga behörigheter.<br>Rutinen bör bygga på att en formell ansökan om behörighet skickas till anställdes chef och/eller systemägare. |

# Sammanställning avvikelser

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.5 | M | Under granskningen noterades det att Svenljunga kommun har ett antal externa leverantörer som har tillgång till systemkonton trots att de endast skall ha personliga konton. | Vid användning av delade konton försämras spårbarheten, vilket ökar risken för att ej tillåtna förändringar i produktionsmiljön utförs och att dessa inte kan knytas till en individ. Detta gör det svårt att i efterhand följa upp vem som har utfört en viss åtgärd. | PwC rekommenderar Svenljunga kommun att se över skapandet av externa leverantörers användarkonton då det framkom att leverantörer har tillgång till systemkonton trots att de endast skall ha personliga konton. |
| 3.5 | M | PwC noterade att Svenbos lösenordspolicy kräver ett 6 tecken långt lösenord vilket är kortare än vad PwC anser är good practice. | Bristfälliga lösenordsparametrar ökar risken för otillåten åtkomst till IT-system, vilket ökar risken för obehörig åtkomst. | PwC rekommenderar bolaget att uppdatera sin lösenordspolicy gällande kravet på antal tecken till minst 8 tecken. |
| 3.5 | M | Under granskningen noterades det att Svenljunga kommun och Svenbo inte genomför en regelbunden granskning av IT-användare eller verksamhetsanvändare för att verifiera att användare i applikationerna har behörigheter som motsvarar deras arbetsuppgifter. | Utan en regelbunden granskning av aktuella behörighetsnivåer ökar risken att användare har behörigheter som inte är aktuella för nuvarande arbetsuppgifter, eller att konton finns kvar efter att personen avslutat sin anställning. Därmed ökar risken för otillbörlig åtkomst och användning av applikationen eller systemet. | PwC rekommenderar Svenljunga kommun och Svenbo att skapa en formell rutin för att minst årligen granska behörigheter med syftet att säkerställa att endast godkända användare har behörighet, samt att dessa användare har korrekt behörighet i applikationer och infrastruktur (operativsystem, servrar och databaser). |

# Sammanställning avvikelser

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.6 | M | Svenbo har i nuläget ett övergripande dokument som beskriver vilka system som uppdateras automatiskt respektive manuellt.<br><br>Svenbo saknar rutin för förändringshantering av system (programförändringar) och det finns inte några kommunicerade krav på kontrollpunkter som bör inkluderas i förändrings-hantering. | Genom att inte ha någon formell och gemensam ändringsrutin för infrastruktur och applikationer ökar risken för felaktiga förändringar i produktionsmiljön som kan påverka hela IT-miljön.<br>Detta kan i slutändan påverka system och applikationers riktighet, konfidentialitet och tillgänglighet. | PwC rekommenderar Svenbo att införa en formell ändringsrutin och kommunicera denna med eventuella berörda leverantörer. Ändringsrutinen bör innehålla:<br>• Formellt godkännande av förändringen<br>• Definierade testkrav<br>• Formellt godkännande innan driftsättning<br>• Reservrutin om ändringen misslyckas<br>• Dokumentationskrav<br><br>Rutinen bör hantera alla typer av förändringar dvs. normala och akuta för både mjuk- och hårdvara och eventuella avsteg från denna bör beskrivas i systemförvaltnings-dokument. Vi rekommenderar även att Svenbo överväger att logga förändringar som utförs i systemen, samt att införa krav på dokumentation av genomförda förändringar. Detta för att möjliggöra uppföljning av att rutinen följs. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.7 | H | Vid granskningen noterades det att Svenbos serverrummet saknar brandlarm, kylaggregat, vattenskydd, UPS och/eller diesel aggregat. | Utan en fullgod fysisk säkerhet ökar risken för skada på utrustning i samband med ex. brand eller vattenläckage. Detta kan medföra störningar i driften av bolagets verksamhet. | PwC rekommenderar Svenbo att se över den fysiska säkerheten i serverrummet med avseende på brandsläckningsutrustning, vattenskydd och skydd mot störningar i elförsörjningen av kritiska servrar genom exempelvis UPS-enheter och/eller diesel-aggregat. |
| 3.8 | L | Svenljunga kommun har en god grund kring upphandlingar av IT-tjänster. Dock noterades att det saknas uppföljning kring krav som ställs i upphandlingar.<br><br>Även Svenbo saknar rutiner för uppföljning av leverantörens tjänster. | Om det inte genomförs återkoppling på att ställda krav uppfylls gentemot leverantör av drift och infrastruktur finns risk att verksamheten inte har den leverans som antas samt att leverantören inte levererar det som bolaget betalar för. | PwC rekommenderar Svenljunga kommun och Svenbo att ställa tydliga krav gentemot leverantören på förväntad leverans inom olika områden gällande exempelvis drift, avbrottsplanerings och infrastruktur. Uppfyllande av dessa krav som finns ska även från leverantörens sida kunna påvisas, exempelvis i rapportform. |

# *Sammanställning avvikelser*

| Om-råde | Prio | Avvikelse | Risk | Rekommendation |
|---|---|---|---|---|
| 3.9 | M | Vid genomgång av Svenljunga kommuns styrande dokument noterades att det inte specificeras att nämndspecifik framtagen dokumentation ska följa kommunövergripande styrande dokumentation. Däremot noterades det vid samtal med personal inom förvaltningarna att de tar hänsyn till kommunövergripande dokumentation vid framtagande av styrande dokument, även om det inte beskrivs i annan dokumentation. | Utan formellt definierade krav på nämndernas implementering av policys och rutiner, och godkännande av avsteg från dessa, finns risk att förväntad nivå på IT-och informationssäkerhet inte finns implementerad. | PwC rekommenderar Svenljunga kommun att upprätta rutiner i styrande dokument för att säkerställa att nämndspecifika styrande dokument adresserar områden kring informations- och IT-säkerhet. Detta genom att tydliggöra vilka krav på informations- och IT-säkerhet som gäller för nämnderna. I detta bör även tydligt ingå vem som kan godkänna avsteg från dessa rutiner och hur denna process sker. |