www.pwc.se

Granskning av IT-säkerhet

Vårgårda och Herrljunga kommuner

April 2018

Anna Lycke Börjesson,
Certifierad kommunal revisor
Elin Jangvik
Vilhelm Kokko

April 2018

pwc

Innehåll

1. Sammanfattning

De förtroende valda revisorerna i Vårgårda kommun och Herrljunga kommun, har gett PwC i uppdrag att genomföra en granskning av IT-säkerhet för att besvara revisionsfrågan:

Har kommunstyrelserna för respektive Herrljunga och Vårgårda kommun samt "Servicenämnd IT, växel och telefoni" gemensamma 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 vår samlade bedömning att IT-säkerheten, ur ett övergripande perspektiv, är tillräcklig för att stödja verksamheten och ge tillräcklig intern kontroll. Dock så finns det att antal områden där Vårgårda kommun och Herrljunga kommun inte har en tillräcklig nivå och IT-säkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll inom IT.

Nedan redovisar vi våra mest väsentliga rekommendationer där vi har bedömt riskerna som höga som respektive kommunstyrelse och Servicenämnd IT, växel och telefoni bör beakta och utvärdera kring åtgärder att prioritera:

- PwC rekommenderar att roller och ansvar avseende IT definieras och kommuniceras och att en formellt ansvarig och uttalad informationssäkerhetsansvarig utses.
- PwC rekommenderar även att rollbeskrivningar förtydligas och att systemägare utpekas för samtliga system.
- PwC rekommenderar att en fullskalig förvaltningsmodell tas fram. En förvaltningsmodell bör innehålla områdena förvaltningsstyrning, användarstöd, ändringshantering och drift och underhåll.
- För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar PwC även att åtgärda de iakttagelser och beakta och åtgärda de rekommendationer som finns beskrivna i appendix.

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 Herrljunga och Vårgårda kommuners revisionsstrategi har kommunerna i sin riskbedömning för 2017 bedömt att en granskning av informations- och IT-säkerheten behöver genomföras. I detta dokument används termen IT-säkerhet för såväl informationssäkerhet som IT-säkerhet. Granskningen genomförs enligt revisionsplanerna 2016/2017 som baseras på de olika riskbedömningarna. Granskningen inleds genom en förstudie vilken beskrivs nedan (benämnd ”granskningen”).

2.2. Syfte och revisionsfråga

Granskningens syfte är att genom en förstudie identifiera risker och behov av en eventuellt fördjupad granskning inom IT-säkerhetsområdet. Detta sker genom en bedömning av kommunstyrelsens dokumenterade rutiner och processer för IT-säkerhet ur ett övergripande perspektiv.

Revisionsfråga:
Har kommunstyrelserna för respektive Herrljunga och Vårgårda kommun samt ”Servicenämnd IT, växel och telefoni” gemensamma 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:

- Kommunallag (1991:900)
- Interna styrdokument
- Internationella standarder enligt ISO (International Organization for Standardization) avseende Informationsteknik, Säkerhetstekniker och Ledningssystem för informationssäkerhet (ISO 27001:2013)
- Internationella standards 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. Inledning

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) med de begränsningar som följer av en förstudie. Granskningen av processer inom IT-säkerhet utfördes genom intervjuer med berörda personer samt granskning av ett urval av relevant dokumentation.

Följande personer har varit intervjuade i granskningen:

Servicenämnd IT, växel och telefoni:
- Jan Pettersson (IT chef)
- Helen Svantesson (processledare IT)
- Mikael Andersson (tjänsteansvarig, IT arkitekt)

Vårgårda kommun:
- Kristina Larsson (systemförvaltare VIVA)

Herrljunga kommun:
- Margareta Ejdestig (systemförvaltare VIVA)

Granskningen har genomförts under februari 2018 av Elin Jangvik (projektledare) och Vilhelm Kokko och kvalitetssäkrad av Anna Lycke Börjesson, samtliga från PwC. Iakttagelserna i rapporten är faktaavstämda med berörd personal.

3. Resultat av granskningen

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

Iakttagelser

Vårgårda kommun och Herrljunga kommun har en central organisation för IT, Servicenämnd IT, växel och telefoni, med framförallt en IT-avdelning för kommunerna. Därtill finns systemförvaltare och systemägare i verksamheterna.

Vid granskningen noterades dock att roller och ansvar inte är tydligt definierat och kommunicerat avseende IT. Det saknas exempelvis en formellt utsedd informationssäkerhetsansvarig och det är inte tydligt vad en systemförvaltare respektive systemägare är ansvarig för. Därtill saknas det en samsyn på vad Servicenämnd IT, växel och telefoni uppdrag är. Det finns olika förväntningar på vad IT ska göra i de olika kommunerna.

Det finns en kort beskrivning av de olika rollerna systemförvaltare och systemägare men detta är inte tillräckligt för att göra rollerna tydliga.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni ej har en tillräcklig nivå gällande styrning av informations- och IT-säkerhet då roller och ansvar inte är tydligt och kommunicerat och att det saknas det en samsyn på vad Servicenämnd IT, växel och telefoni uppdrag är och det finns olika förväntningar på vad Servicenämnd IT, växel och telefoni ska göra i de olika kommunerna.

PwC rekommenderar att roller och ansvar avseende IT definieras och kommuniceras och att en formellt ansvarig och uttalad informationssäkerhetsansvarig utses. PwC rekommenderar att rollbeskrivningar förtydligas och att systemägare utpekas för samtliga system.

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

Både Vårgårda och Herrljunga kommuner har ett antal styrande dokument såsom policys och användarinstruktioner som är föråldrade och inte har anpassats efter de förändringar som skett över de senaste åren. Det pågår för närvarande ett arbete med att ta fram nya policydokument och riktlinjer.

Servicenämnd IT, växel och telefoni saknar i dagsläget en förvaltningsmodell för hur förvaltningsstyrning, användarstöd, ändringshantering och drift och underhåll ska hanteras.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni i nuläget ej har en tillräcklig nivå gällande styrande dokument då ej samtliga policys och rutinbeskrivningar är formellt antagna och en tydlig förvaltningsmodell saknas.

PwC rekommenderar att det påbörjade arbetet med genomgång av policys och instruktioner fortsätter, och att formerna sätts för hur en förvaltningsmodell skall se ut för Servicenämnd IT, växel och telefoni. I nästa steg bör uppföljning av implementering och efterlevnad genomföras.

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 hantera nya risker och hot?

Iakttagelser

Kommunerna har identifierat de mest verksamhetskritiska systemen samt använt sig utav programmet KLASSA för att identifiera risker och sårbarhet för dessa system. Det har dock inte gjorts någon formell och dokumenterad risk- och sårbarhetsanalys på övergripande nivå för Servicenämnd IT, växel och telefoni och ej verksamhetskritiska system har inte utvärderats i KLASSA.

Servicenämnd IT, växel och telefoni hanterar säkerhetskopiering och återläsningstest, dock är frekvenserna för detta inte kommunicerat och förankrat med verksamheten. Verksamheten har inte definierat vilka krav för systemens tillgänglighet som skall gälla och det saknas policy och rutinbeskrivningar gällande rutinerna kring säkerhetskopiering.

För delar av verksamheten finns det krisplaner vilka detaljerar hur man skall fortsätta arbeta utan systemstöd i händelse av ett avbrott. Vi noterade dock att det saknas formellt dokumenterade krisplaner för delar av verksamheten.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni i nuläget i stort har en tillräcklig nivå gällande rutiner för att identifiera och hantera risker och hot då riskanalyser har utförts för de mest verksamhetskritiska systemen, säkerhetskopiering sker och det finns krisplaner för delar av verksamheten.

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar PwC dock att de iakttagelser som finns beskrivna i område 3.3 i appendix åtgärdas samt att respektive rekommendation beaktas.

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

Incidenter rapporteras in till Servicenämnd IT, växel och telefoni som registrerar dessa i sitt ärendehanteringssystem och arbetar med att lösa incidenterna.

Processen för hur incidenter hanteras finns beskriven men processen följs inte alltid och det saknas en rutin för uppföljning/mätning på lösta/olösta problem.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni har en tillräcklig nivå gällande incidenthantering då det finns en process för hur de ska arbeta.

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar PwC dock att de iakttagelser som finns beskrivna i område 3.4 i appendix åtgärdas samt att respektive rekommendation beaktas.

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

Båda kommunerna har rutiner för behörighetsadministration men dessa är bristfälliga samt skiljer sig åt mellan både kommunerna och systemen.

Därtill saknas rutiner för uppföljning utav tilldelade behörigheter även om man för vissa system ser över licenserna kontinuerligt för att säkerställa att man betalar licensavgifter för rätt antal användare.

Kommunerna har lösenordspolicys i sina respektive användarinstruktioner men dessa följs inte fullt ut både gällande AD, Novell och verksamhetssystem.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni i stort har en tillräcklig nivå gällande behörighetshantering för kommungemensamma system då det finns rutiner för upplägg och ändring på plats.

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar PwC dock att de iakttagelser som finns beskrivna i område 3.5 i appendix åtgärdas samt att respektive rekommendation beaktas.

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

Servicenämnd IT, växel och telefoni arbetar enligt ITIL i ärendehanteringssystemet Nilex och det finns en changegruppering inom Servicenämnd IT, växel och telefoni. Arbetssättet är under utveckling och vid granskningstillfället noterades att det i dagsläget inte finns någon rutinbeskrivning för förändringshantering av system (programförändringar) och det finns inte några definierade och kommunicerade krav på kontrollpunkter som bör inkluderas i förändringshantering.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni i stort har en tillräcklig nivå gällande hantering av programförändringar då informella rutiner för hantering av förändringar finns på plats, dock är dessa inte dokumenterade

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar PwC dock att de iakttagelser som finns beskrivna i område 3.6 i appendix åtgärdas samt att respektive rekommendation beaktas.

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

Inom kommunerna finns det sedan november en gemensam serverhall i kommunhuset i Herrljunga som Servicenämnd IT, växel och telefoni är ansvariga för. Serverhallen har bland annat inpasseringsskydd, temperatur- och fuktövervakning och skydd mot bortfall i elförsörjning (UPS och dieselaggregat). Till serverutrymmen är det enbart IT-avdelningen som har tillgång.

Det finns även en datahall i Vårgårda där backuper förvaras.

Vid granskningen noterades det att det inte görs inte någon periodisk genomgång av fysiska behörigheter (ex behörigheter in till serverhall) för att säkerställa att enbart personer som har ett behov i sina arbetsuppgifter att få åtkomst till känsliga områden har denna behörighet.

Det sker heller ingen uppföljning av inpassering till kommunens driftlokaler. Leverantörer som gör underhåll på servrar, UPS och dieselaggregat släpps in i driftlokaler och övervakas inte. Vid granskningen stod dörrarna öppna in till dessa lokaler för att leverantör arbetade med underhåll.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni i stort 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 risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar PwC dock att de iakttagelser som finns beskrivna i område 3.7 i appendix åtgärdas samt att respektive rekommendation beaktas.

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

Det finns en upphandlingsansvarig för båda kommunerna som även är involverad i IT-inköp. Därtill ska Servicenämnd IT, växel och telefoni verka samordnande för att effektivisera IT-inköp.

Servicenämnd IT, växel och telefoni ansvarar för driften av IT-miljön och använder sig inte av outsourcingleverantörer. Verksamheterna har vissa system där de tar hjälp av outsourcingleverantörer och vi noterade vid granskningstillfället att det saknas avtal med outsourcingleverantörer för vissa av de system som verksamheterna använder.

Därtill saknas serviceavtal mellan kommunerna och Servicenämnd IT, växel och telefoni och det görs inte någon uppföljning för att säkerställa att de uppfyller de krav verksamheten har gällande förväntad leverans.

Bedömning

Vår bedömning är att respektive kommunstyrelse och Servicenämnd IT, växel och telefoni i stort har en tillräcklig nivå gällande outsourcing och upphandlingar kopplat till IT.

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar PwC dock att de iakttagelser som finns beskrivna i område 3.8 i appendix åtgärdas samt att respektive rekommendation beaktas.

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

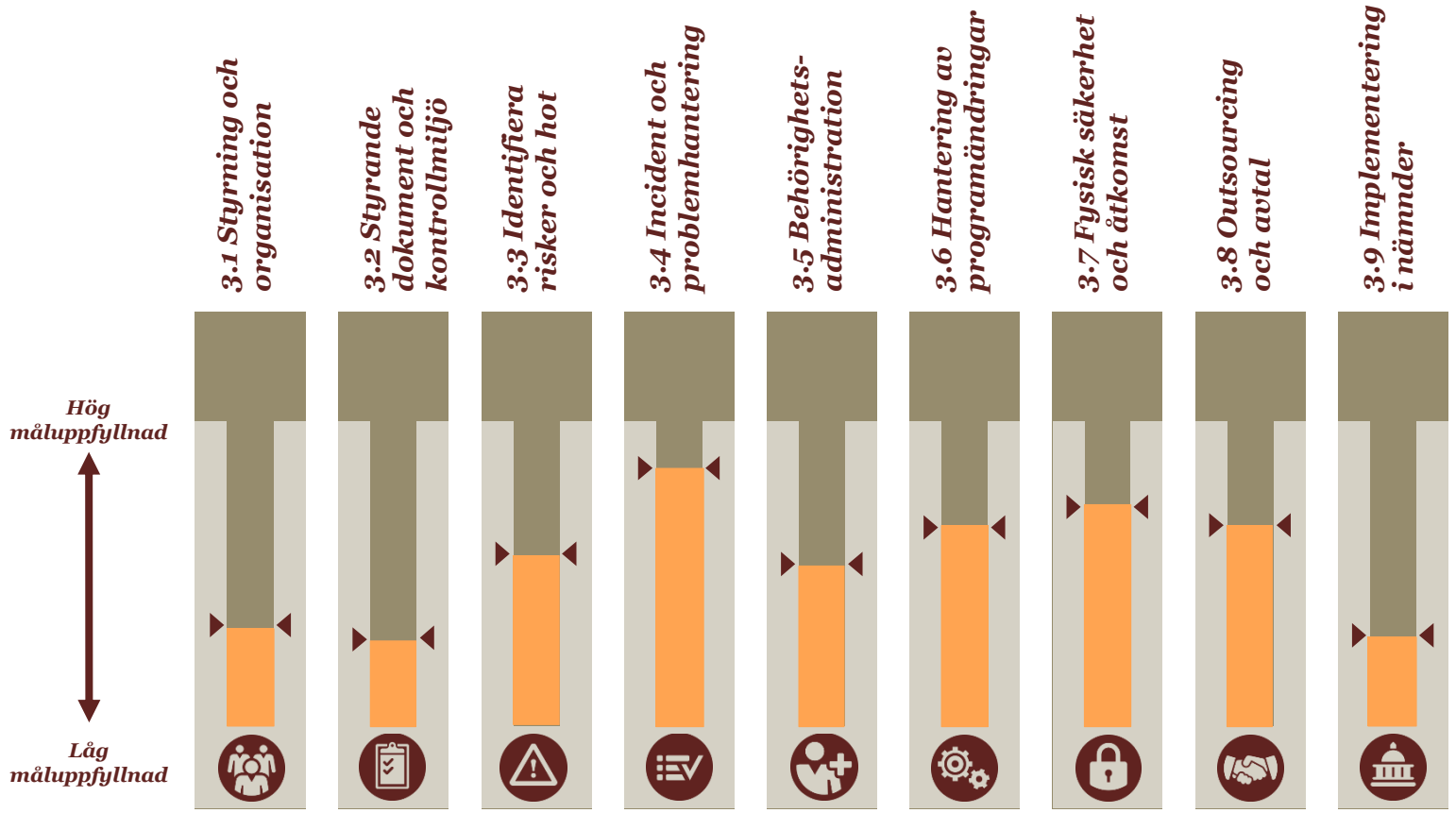
De styrande dokument som finns inom Vårgårda och Herrljunga kommun är på kommunövergripande nivå. För iakttagelser och bedömningar se svar på 3.1 och 3.2 ovan.

Bedömning

För iakttagelser och bedömningar se svar på 3.1 och 3.2 ovan.

4. Sammanfattande mognadsgrad per kontrollmål

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



Datum: 2018-04-20

Elin Jangvik
Projektledare

Vilhelm Kokko
Projektmedlem

Fredrik Carlsson
Uppdragsledare

Anna Lycke Börjesson
Kvalitetssäkrare

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 över den finansiella rapporteringen.
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 att roller och ansvar inte är tydligt definierat och kommunicerat avseende IT. Det saknas exempelvis en formellt utsedd informationssäkerhetsansvarig och det är inte tydligt vad en systemförvaltare respektive systemägare är ansvarig för. Därtill saknas det en samsyn på vad Servicenämnd IT, växel och telefoni uppdrag är. Det finns olika förväntningar på vad IT ska göra i de olika kommunerna. Det finns en kort beskrivning av olika rollerna systemförvaltare och systemägare men detta är inte tillräckligt för att göra rollerna tydliga.	För att kunna skapa och bibehålla tillräcklig kontroll över kommunernas information och för att säkerställa välgrundade prioriteringar är det viktigt att utse en person med ett formellt övergripande informationssäkerhetsansvar. Det är viktigt att tydliggöra vad Servicenämnd ITs uppdrag omfattar så att det inte blir ett förväntansgap. Utan tydligt definierade och formaliserade roller avseende ansvar av IT-systemen finns det en risk att systemförvaltningen inte styrs på ett effektivt sätt, exempelvis att väsentliga beslut ej tas av korrekt person eller av informationssäkerhetsfrågor inte hanteras i den utsträckning som krävs.	Vi rekommenderar att roller och ansvar avseende IT definieras och kommuniceras och att en formellt ansvarig och uttalad informationssäkerhetsansvarig utses. Den som är ansvarig för informationssäkerheten kommer att ha en viktig roll i att definiera, bibehålla samt kommunicera de informationssäkerhetskrav som kommunerna har. Därtill bör Servicenämnd IT, växel och telefoni ansvarsområden tydliggöras och kommuniceras. Vi rekommenderar även att kommunerna tydligt beskriver vad systemförvaltare respektive systemägare har för ansvar. Detta ansvar kan med fördel dokumenteras i samband med upprättandet av övriga styrande dokument för organisationen. I komplement till detta bör det finns tydliga rollbeskrivningar. Detta bör även kommuniceras till respektive person.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.1	M	Det finns ett högt beroende av nyckelpersoner i kommunerna avseende IT-organisationen. Detta på grund av att IT-organisationen i mångt och mycket saknar instruktioner och rutinbeskrivningar relaterat till exempelvis behörighetshantering, ändringshantering, avbrottsplan, kontinuitetsplan samt IT-arkitektur.	Ett högt personberoende av nyckelpersoner ökar risken för att kompetens försvinner om nyckelperson väljer att sluta., vilket i sin tur ökar risken för att väsentliga arbetsmoment inte utförs på ett ändamålsenligt sätt.	Vi rekommenderar Servicenämnd IT, växel och telefoni att upprätta instruktioner och rutinbeskrivningar, framförallt relaterat till behörighetshantering, ändringshantering samt IT-arkitektur, för att säkerställa att nuvarande kompetens i IT-organisationen kan tillvaratas av andra personer än nuvarande nyckelpersoner.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.1	L	Det noterades vid granskningen att kommunerna saknar regelbundna utbildningar avseende IT-säkerhet, och uppföljning av dessa, för exempelvis nyanställda och systemförvaltare.	Utan regelbundna utbildningar och uppföljning av dessa finns det en risk att anställda saknar relevant kunskap om sin roll och sitt ansvar, vilket i sin tur ökar risken för att systemförvaltningen inte styrs på ett effektivt sätt och att viktiga arbetsmoment uteblir eller utförs på ett felaktigt sätt.	Vi rekommenderar att Servicenämnd IT, växel och telefoni och kommunerna implementerar regelbunden utbildning, framförallt för nyanställda och systemförvaltare, för att säkerställa att det finns gedigen och uppdaterad kompetens gällande roller och ansvar ute i verksamheterna.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	M	Det noterade vid granskningen att samtliga policys och användarriktlinjer gällande IT inom kommunerna är föråldrade och inte har anpassats efter de förändringar som skett över de senaste åren. Det pågår för närvarande ett arbete med att ta fram nya policydokument och riktlinjer. Vidare noterades det att det heller inte finns någon rutin för att uppdatera styrdokument, kommunicera dessa eller följa upp dess efterlevnad.	Avsaknad av en aktuella policy-dokument försvårar styrningen av verksamheten och kan leda till onödiga kostnader genom sämre grundade beslut av IT-investeringar och resursallokering.	Det finns enligt Servicenämnd IT, växel och telefoni utkast framtaget på policydokument och riktlinjer för hur den ska brytas ner och vi rekommenderar att dessa färdigställs och antas. Policydokumenten skall återspegla dagens förutsättningar och blicka framåt. Vikt bör läggas på att kommunicera och förankra innehållet samt att hålla det levande över tiden och följa upp efterlevnad.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	M	Det finns vissa rutiner på plats för hur Servicenämnd IT, växel och telefoni ska arbeta men vi noterade under granskningen att det saknas ett ramverk för intern kontroll avseende IT.	Utan ett formellt kontroll-ramverk finns risken att implementerade rutiner och kontroller inte lever upp till kommunernas behov (exempelvis informationssäkerhetskrav).	Vi rekommenderar Servicenämnd IT, växel och telefoni att ta fram ett formellt ramverk för vilka IT kontroller som skall finnas på plats inom de olika processerna. Inom ramen för detta bör det även inkluderas rutiner gällande uppföljning av dessa kontroller.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	H 	Servicenämnd IT, växel och telefoni saknar i dagsläget en förvaltningsmodell.	Avsaknad av en tydlig förvaltningsmodell kan orsaka att IT-stödet inte ger avsedd nytta i verksamheten eller att styrningen försvåras där många parter är involverade. Det kan också skapa avsaknad av tydliggjorda roller och ansvar.	Vi rekommenderar Servicenämnd IT, växel och telefoni att ta fram en fullskalig förvaltningsmodell. En förvaltningsmodell bör innehålla områdena förvaltningsstyrning, användarstöd, ändringshantering och drift och underhåll, exempelvis: • Definierade roller och ansvar för systemet (samt ansvarsfördelning mellan Servicenämnd IT, växel och telefoni och förvaltningar) • Riskanalys • Systemmiljö • Informationssäkerhetskrav • Systemspecifika rutinbeskrivningar och kontroller • Krav på tillgänglighet och säkerhetskopiering

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	L	Det finns en sammanställning över alla system inom de två kommunerna där bland annat systemägare och systemförvaltare pekas ut. Detta är ett levande dokument som tas upp som en stående punkt i ett leveransforum. Sammanställningen är dock inte uppdaterad och det saknas i filen utpekade systemförvaltare och systemägare för flera system.	Utan tydligt definierade och formaliserade roller avseende ansvar av IT-systemen finns det en risk att systemförvaltningen inte styrs på ett effektivt sätt, exempelvis att väsentliga beslut ej tas av korrekt person eller av informationssäkerhetsfrågor inte hanteras i den utsträckning som krävs.	Vi rekommenderar Servicenämnd IT, växel och telefoni att ta uppdatera sammanställningen över alla system och säkerställa att alla system, inklusive driftssystem, har en utpekad systemägare och systemförvaltare.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	M	Det noterades att kommunerna har identifierat de mest verksamhetskritiska systemen samt använt sig utav programmet KLASSA för att identifiera risker och sårbarhet för dessa system. Det har dock inte gjorts någon formell och dokumenterad risk- och sårbarhetsanalys på övergripande nivå för Servicenämnd IT, växel och telefoni och ej verksamhetskritiska system har inte utvärderats i KLASSA.	Att inte regelbundet genomföra riskanalyser för verksamheten där risker och hot identifieras kan medföra att risker förbises som kan medföra skada för kommunerna.	Vi rekommenderar att en övergripande risk och sårbarhetsanalys för Servicenämnd IT, växel och telefoni utförs där risker utvärderas. En riskanalys som täcker in flertalet IT-relaterade risker gör kommunerna bättre förberett vid en eventuell incident och kan ge indikationer på vilka åtgärder som krävs för att stärka kontroller och rutiner. Som en del i detta bör information klassificeras baserat på konfidentialitet, riktighet och tillgänglighet.
3.3	M	Verksamheten har inte definierat vilka krav för systemens tillgänglighet (exempelvis maximal ned-tid och hur lång tid det får gå mellan säkerhetskopiering) som skall gälla. Servicenämnd IT, växel och telefoni hanterar säkerhetskopiering och återläsningstest, dock är frekvenserna för detta inte kommunicerat och förankrat med verksamheten.	Avsaknad av tydliga krav, samt avsaknad kring återkoppling på att dessa krav uppfylls för kommunernas system, kan innebära en risk att tillgänglighet och återläsningsmöjligheter inte uppfyller verksamheten krav.	Vi rekommenderar Servicenämnd IT, växel och telefoni att inhämta krav från verksamheten kring vilka systemspecifika krav som skall gälla för tillgänglighet och återläsning. Detta bör exempelvis definieras i förvaltningsbeskrivning för respektive system.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	M	Det saknas policy och rutinbeskrivningar gällande rutinerna kring säkerhetskopiering.	Avsaknad av säkerhetskopieringspolicy innebär att kommunerna är beroende av kunskapen och rutinerna hos särskilda nyckelpersoner och utan dessa riskerar arbetet med säkerhetskopieringen att fallera.	Vi rekommenderar Servicenämnd IT, växel och telefoni att upprätta en policy för säkerhetskopiering samt dokumentera rutinerna kring säkerhetskopieringen. Information bör inhämtas från verksamheterna avseende systemens säkerhetsmål och kontinuitetsplanering för att säkerställa att verksamhetens krav på tillgänglig data uppnås. Dokumentationen bör innefatta vilka system som omfattas av säkerhetskopiering och frekvens för dessa, samt att återläsning sker av kritiska system baserat på en genomförd riskanalys (baserat på verksamhetens krav). Krav på återläsning skall dokumenteras för att säkerställa att genomförande och kvalitet överensstämmer med verksamhetens krav på tillgängliga data. Säkerhetskopior skall även förvaras på lämpligt sätt och finnas tillgängliga under avtalad tidsperiod.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	M	Vi noterade under granskningen att man för delar av verksamheten tagit fram krisplaner vilka detaljerar hur man skall fortsätta arbeta utan systemstöd i händelse av ett avbrott. Vi noterade dock att det saknas formellt dokumenterade krisplaner för delar av verksamheten.	Avsaknad av dokumenterade planer 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 (krisplanering) leder även till en ökad risk för att verksamheten blir utan systemstöd längre än nödvändigt samt att verksamheten avstannar helt vid systembortfall.	Vi rekommenderar kommunerna att dokumentera de åtgärder som behöver vidtas, i vilken ordning och av vem, för att effektivt återställa system och applikationer vid en eventuell incident. Ansvarsområden bör beskrivas och kommuniceras till alla berörda, exempelvis genom träning samt testning av planen. Krisplanerna bör vidare stämmas av med eventuella leverantörer så att de återställningskrav som definierats reflekteras av de servicekontrakt som finns.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.4	L	Vid granskning noterades det att verksamheten inte alltid följer den process som finns på plats när det gäller incidenthantering samt att de inte har någon rutin på plats för uppföljning/mätning på lösta/olösta problem.	Om resurser inte avsätts till att lösa problem och dessa fel-prioriteras, kan det leda till omotiverade kostnader eller oväntade störningar.	Vi rekommenderar Servicenämnd IT, växel och telefoni att se över rutinen för incident/problemhantering och följer upp efterlevnad av rutinen. En sådan rutin bör innehålla en tydlig mottagare av incidentlarm, hanteringsregler för olika typer av incidenter, ett verktyg för att samla alla incidenter (inklusive driftslarm), instruktioner för eventuell eskalering av ärenden och en utpekad ansvarig för dessa aktiviteter.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.5	M	Vi noterade under granskningen att båda kommuner har rutiner för behörighetsadministration (dvs. nybeställning, ändring och borttag av behörigheter) men att dessa är bristfälliga samt skiljer sig åt mellan både kommunerna och systemen. Vi noterade även under granskningen att det saknas rutiner för uppföljning utav tilldelade behörigheter även om man för vissa system ser över licenserna kontinuerligt för att säkerställa att man betalar licensavgifter för rätt antal användare.	Avsaknad av definierade rutiner kring behörighetsadministration kan medföra ett antal risker. Risken för direkta obehöriga förändringar i systemen ökar om det finns användare med för höga eller felaktiga behörigheter samtidigt som risken för obehörig åtkomst ökar när användarkonton finns kvar efter anställnings upphörande. Utan en regelbunden granskning av aktuella behörighetsnivåer ökar risken att användare har behörigheter som inte är aktuella för nuvarande arbetsuppgifter, eller att personen slutat vid företaget. Därmed ökar risken för otillbörlig åtkomst och användning av applikationen eller systemet.	Vi rekommenderar att rutinerna kring behörighetsadministration formaliseras. Alla steg i behörighetsadministrationen (dvs. nybeställning, ändring och borttag av behörigheter) bör dokumenteras och arkiveras. Vi rekommenderar att en formell rutin utformas för att regelbundet granska behörigheter för att säkerställa att användare i applikationerna och underliggande system har behörigheter som motsvarar arbetsuppgifter. Genomgången bör dokumenteras och sparas.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.5	M	Vi noterade under granskningen att kommunerna har lösenordspolicys i sina respektive användarinstruktioner men att kommunerna inte följer sina egna policys fullt ut både gällande AD och Novell men även verksamhetssystem. Exempelvis stämmer inte faktisk periodicitet för lösenordsbyte i AD och Novell med definierade krav i lösenordspolicys, krav på komplexitet är inte påslaget för den ena kommunen och faktiskt krav på lösenordslängd är för kort enligt PwCs god praxis.	Bristfälliga lösenordsparametrar ökar risken för otillåten och obehörig åtkomst till finansiella applikationer. Att lösenordsparametrarna inte följer den uppsatta policyn gör att risken för otillåten åtkomst till systemen ökar.	Vi rekommenderar Servicenämnd IT, växel och telefoni och systemförvaltare att genomföra regelbundna genomgångar av lösenordssättningarna för att säkerställa att de är i linje med den upprättade policyn. Vi rekommenderar även att lösenordskraven för både för Active Directory, Novell och verksamhetssystem utvärderas för att säkerställa att dessa är på en mer lämplig nivå.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.6	M	Servicenämnd IT, växel och telefoni arbetar enligt ITIL i ärendehanteringssystemet Nilex och det finns en changegruppering inom Servicenämnd IT, växel och telefoni. Arbetssättet är under utveckling och vid granskningstillfället noterades att det i dagsläget inte finns någon rutinbeskrivning för förändringshantering av system (programförändringar) och det finns inte några definierade och 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. Detta kan i slutändan påverka system och applikationers riktighet, sekretess och tillgänglighet.	Vi rekommenderar Servicenämnd IT, växel och telefoni att dokumentera en formell ändringsrutin och kommunicera denna med eventuella berörda personer inom kommunerna och leverantörer. Ändringsrutinen bör innehålla åtminstone: • Formellt godkännande av förändringen • Definierade testkrav • Formellt godkännande innan driftsättning • Reservrutin om ändringen misslyckas • Dokumentationskrav 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 också att kommunerna överväger att logga förändringar som utförs i systemen, samt att införa gemensamma krav på dokumentation. Detta för att möjliggöra uppföljning av att rutinen följs.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.6	L	Konsulter ska generellt släppas in på servrar av Servicenämnd IT, växel och telefoni vid behov. Det finns dock leverantörer för vårdsystem som har ständig access men som ska informera om att de loggar in på servrarna. Det saknas i dagsläget en uppföljning av konsulternas användaraktiviteter.	Avsaknad av rutiner kring uppföljning av loggar kan medföra att felaktigheter och obehörig åtkomst inte upptäcks i tid, alternativt inte upptäcks alls.	Vi rekommenderar att konsulters användaraktiviteter följs upp regelbundet för att säkerställa att dessa ligger inom förväntan.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.6	L	Vid vår granskning blev vi informerade om att det inte finns rutiner för att erhålla uppdaterad systemdokumentation för samtliga verksamhetssystem.	Att inte ha uppdaterad och tillförlitlig systemdokumentation för känsliga system kan medföra att systemet blir otillgängligt under en alltför lång tid om något går fel. Den detaljerade kunskapen om hur felet skall korrigeras kanske inte finns tillgänglig vid det aktuella tillfället. Detta kan få kostsamma konsekvenser och leda till ett ökat personberoende.	Vi rekommenderar att kommunerna säkerställer att de har åtkomst till uppdaterad systemdokumentation för samtliga verksamhetskritiska system. Systemförvaltare för respektive system bör ansvara för dokument och se till att det hålls uppdaterat. Dokumenten bör förvaras på ett säkert ställe skyddat mot brand och stöld.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.7	L	Vid inspektion utav serverutrymmet hos Herrljunga kommun noterades att det finns mindre brister i säkerheten. Det saknas lås till rummet för dieselgenerator samt att det finns brandfarligt material i serverrummet.	Utan en fullgod fysisk säkerhet i de rum där dator- och kommunikationsutrustning förvaras riskeras att utrustningen eller personal skadas vid t.ex. brand. Avsaknaden utav lås till rum med dieselgeneratorn ökar även risken för oavsiktlig eller avsiktlig skada på utrustningen.	Vi rekommenderar Servicenämnd IT, växel och telefoni att se över möjligheten att införskaffa tillträdesskydd till utrymmet med dieselgenerator samt att inte förvara brandfarligt material som hyllor i trä i serverutrymmet.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.7	M	Vid granskningen noterades det att det inte görs inte någon periodisk genomgång av fysiska behörigheter (ex behörigheter in till serverrum) för att säkerställa att enbart personer som har ett behov i sina arbetsuppgifter att få åtkomst till känsliga områden har denna behörighet. Det sker heller ingen uppföljning av inpassering till driftlokaler. Leverantörer som gör underhåll på servrar, UPS och dieselaggregat släpps in i driftlokaler och övervakas inte. Vid granskningen stod dörrarna öppna in till dessa lokaler för att leverantör arbetade med underhåll.	Avsaknad av en formellt kontroll för att fastställa vilka/hur många anställda hos Servicenämnd IT, växel och telefoni som har fysisk åtkomst till serverrum etc. ökar risken för obehörighet åtkomst. Det finns exempelvis en risk för att någon av misstag skadar kritiska system (t ex kommer åt sladdar eller stänger av servrar) eller avsiktligen missbrukar detta för att komma åt kritiska system eller information.	Vi rekommenderar att Servicenämnd IT, växel och telefoni ser över vilka som har åtkomst till serverrummet och begränsare antalet så att endast beviljas ett fåtal personer som utifrån sina arbetsuppgifter behöver ha tillträde till serverrummet. Vidare rekommenderar vi att Servicenämnd IT, växel och telefoni regelbundet följer upp vilka som har tillgång till och har varit inne i serverrummet för att säkerställa att rätt personer har åtkomst över tid.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.8	M 	Servicenämnd IT, växel och telefoni ansvarar för driften av IT-miljön och använder sig inte av outsourcingleverantörer. Verksamheterna har vissa system som där de tar hjälp av outsourcingleverantörer och vi noterade vid granskningstillfället att det saknas avtal med outsourcingleverantörer för vissa av de system som verksamheterna använder. Därtill saknas serviceavtal mellan kommunerna och Servicenämnd IT, växel och telefoni och det görs inte någon uppföljning för att säkerställa att de uppfyller de krav verksamheten har gällande förväntad leverans.	Utan dokumenterade avtal med leverantörer finns en risk för att säkerhetsnivån inte är anpassad efter verksamhetens krav, samt att verksamheten drabbas vid eventuella oklarheter i muntliga överenskommelser.	Vi rekommenderar att kommunerna säkerställer att avtal och SLA finns med sina outsourcingleverantörer. Vidare rekommenderar vi att verksamheten ställer tydliga krav gentemot leverantören på förväntad leverans inom olika områden gällande drift, avbrottsplanering och infrastruktur samt att uppfyllande av bör följas upp regelbundet. Därtill rekommenderar vi Servicenämnd IT, växel och telefoni att upprätta serviceavtal med kommunerna.