FALKENBERG
REVISORERNA

Datum 2018-04-12

Kommunstyrelsen

Kommunfullmäktige – för kännedom

Granskning av IT- och informationssäkerhet
Revisorerna i Falkenbergs kommun har gett PwC i uppdrag att genom en förstudie granska om kommunstyrelsen har *ändamålsenliga policys, rutiner och beskrivningar gällande IT-säkerhet, med fokus på design av rutiner för skydd mot obehörig åtkomst av data och information?*

Vår bedömning
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 Falkenbergs kommun inte har en tillräcklig nivå och IT-och informationssäkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll inom IT.

Vi baserar vår bedömning på genomgången av de kontrollmål vilka redovisas i bifogad revisionsrapport.

Våra rekommendationer är:

- Vi rekommenderar kommunstyrelsen att se över och uppdatera nuvarande policydokument för att säkerställa att dessa är aktuella och återspeglar kommunens verksamhet, samt införa rutiner där styrdokument ses över och uppdateras regelbundet, förslagsvis en gång per år.

- Vi rekommenderar kommunstyrelsen att utvärdera vilka kontrollpunkter som skall följas upp med viss periodicitet med Evry. Exempelvis bör uppföljningen inkludera genomförda tester av avbrottsplan, återläsningstester av backuper, efterlevnad av behörighetshanteringskontroller och förändringshanteringskontroller.

- För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT-och informationssäkerhet rekommenderar vi även kommunstyrelsen att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i appendix i bifogad rapport.

I övrigt hänvisar vi till granskningsrapporten som bifogas i bilaga: PwC Revisionsrapport *"Granskning av IT- och informationssäkerhet"*.

Vi önskar era kommentarer senast 2018-08-30. Svar skickas till kommunrevisionen; gosta.svensson@pol.falkenberg.se

Falkenberg den 12 april 2018

.....
Gösta Svensson

.....
Jan Johansson

Bilaga: Revisionsrapport PwC " *Granskning av IT- och informationssäkerhet*"

www.pwc.se

Granskning av IT- och informationssäkerhet

Falkenbergs kommun

Februari 2018

Kajsa Jansson
Julia Lahti

Februari 2018

pwc

Innehåll

1. Sammanfattning

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

Har kommunstyrelsen 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 Falkenbergs kommun inte har en tillräcklig nivå och IT- och informationssäkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll inom IT.

Nedan redovisar vi våra mest väsentliga rekommendationer som kommunstyrelsen bör beakta och utvärdera kring åtgärder att prioritera:

- PwC rekommenderar Falkenbergs kommun att se över och uppdatera nuvarande policydokument för att säkerställa att dessa är aktuella och återspeglar kommunens verksamhet, samt införa rutiner där styrdokument ses över och uppdateras regelbundet, förslagsvis en gång per år.
- PwC rekommenderar Falkenbergs kommun att utvärdera vilka kontrollpunkter som skall följas upp med viss periodicitet med Evry. Exempelvis bör uppföljningen inkludera genomförda tester av avbrottsplan, återläsningstester av backuper, efterlevnad av behörighetshanteringskontroller och förändringshanterings-kontroller.
- För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi även Falkenbergs kommun att åtgärda de iakttagelser och beakta 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 Falkenbergs kommuns revisionsstrategi har kommunens 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 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.

Granskningen syftar till att besvara följande övergripande revisionsfråga:

Har kommunstyrelsen 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) 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:

- Thorbjörn Larsson (IT-chef)
- Lena Davidsson (Informationssäkerhetssamordnare)
- Birgitta Lomander Johansson (IT-utvecklingschef, Soc)
- Jonas Brännström (Systemutvecklare, Soc)
- Carolina Ghafari (IT-samordnare, Soc).

Granskningen har genomförts under februari 2018 av Kajsa Jansson (projektledare) och Julia Lahti, båda från PwC. Rapporten har kvalitetssäkrats av Fredrik Carlsson (uppdragsledare). Rapporten är faktaavstämd med berörd personal.

3. Resultat av granskningen

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

Iakttagelser

Falkenbergs kommun har en central organisation för IT, samt en informationssäkerhetssamordnare som arbetar med intern kontroll och dataskyddsförordningen. IT-enheten ansvarar bland annat för stöd i upphandlingsprocessen för IT, teknisk support samt implementation av nya system. Roller och ansvar för IT- och informationssäkerhet finns, på en övergripande nivå, beskrivet i riktlinjerna för informationssäkerhet.

Vid granskningen noterades att Falkenbergs kommun saknade detaljerade riktlinjer som säkerställer att IT- och informationssäkerhet hanteras på ett ändamålsenligt sätt i nämnderna.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande styrning av informations- och IT-säkerhet då det finns tydliga roller och ansvar, samt att dessa är definierade i formella riktlinjer för informationssäkerhet.

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi dock Falkenbergs kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.1 i appendix.

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

Falkenbergs kommun har ett antal styrande dokument för IT- och informationssäkerhet inom kommunen, såsom IT-strategi, Informationssäkerhetspolicy och Användarinstruktioner.

Vid granskningstillfället så noterades det att relevanta policydokument, såsom IT-strategi och Informationssäkerhetspolicy, inte uppdaterats på 8-18 år. Vidare saknas en rutin som säkerställer att dessa policydokument regelbundet ses över och uppdateras för att återspegla kommunens verksamhet.

Bedömning

Vår bedömning är att kommunen i nuläget ej har en tillräcklig nivå gällande styrande dokument då flertal styrande dokument inte uppdaterats på 8-18 år och riskerar att inte återspegla Falkenbergs kommuns verksamhet, samt att det inte finns någon rutin på plats som säkerställer att policydokument uppdateras regelbundet.

Vi rekommenderar Falkenbergs kommun att se över och uppdatera nuvarande policydokument för att säkerställa att dessa är aktuella och återspeglar kommunens verksamhet, samt införa rutiner där styrdokument ses över och uppdateras regelbundet, förslagsvis en gång per år.

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

Falkenbergs kommun har genomfört en risk- och sårbarhetsanalys. Respektive nämnd ansvarar för att analysera och vidta åtgärder baserat på utfallet. Baserat på intervju med utvald nämnd så noterades det att nämnden identifierat kritiska system och har använt sig av Klassa för vidare analys.

Vid granskningstillfället noterades det dock att Falkenbergs kommun saknar riktlinjer och instruktioner för genomförande av riskanalyser samt identifiering av kritiska processer och system, så att detta sker på ett likformigt och ändamålsenligt sätt i nämnderna.

Vidare så har verksamheten inte definierat vilka specifika krav för systemens tillgänglighet (exempelvis upptid och återläsningskrav baserat på genomförda riskanalyser) som skall gälla.

Leverantör Evry hanterar avbrottsplan, säkerhetskopiering och återläsningstest, dock är frekvenserna för detta inte kommunicerat och förankrat med verksamheten.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande rutiner för att identifiera och hantera risker och hot då kommunen har genomfört en risk- och sårbarhetsanalys, samt för att nämnderna analyserat och vidtagit åtgärder baserat systemspecifika riskanalyser.

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi dock Falkenbergs kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.3 i appendix.

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

Falkenbergs kommun har outsourcat problem- och incidenthantering till Evry, vilket är reglerat i nuvarande Service Level Agreement (SLA). Samtliga slutanvändare inom kommunen kan rapportera incidenter och problem till Evry via Evrys egna ärendehanteringssystem och det finns en rutin på plats för övervakning av aktiviteter i kommunens nätverk.

Samtliga som arbetar med incident- och problemhantering är certifierade enligt ITIL. Evry och IT- chef har veckomöten gällande lösning av incidenter och månadsmöten gällande aktuell statistik över incident- och problemhantering.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande incidenthantering då det finns en upparbetad rutin och ett ärendehanteringssystem som säkerställer att incidenter och problem hanteras. Uppföljning sker även i form av driftsmöten för att informera kommunen om nuläge. Vid granskningen noterades inga iakttagelser kopplat till kontrollmålet.

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

Falkenbergs kommuns behörighetshantering skiljer sig åt beroende på om det gäller åtkomst till nätverk och filstruktur (Active Directory), kommungemensamma system eller verksamhetssystem. Evry har en formaliserad rutin för tilldelning, ändring och borttag av behörigheter för Active Directory och kommungemensamma system där beställningar stäms av mot personalsystem och gällande behörighetslista som attesterats av förvaltningschef. Behörigheter till verksamhetssystemen hanteras inom respektive nämnd av systemförvaltare.

Vid granskningstillfället noterades det att inga rutinbeskrivningar eller riktlinjer är upprättade på övergripande nivå för att stötta nämnderna gällande grundkrav för hantering av behörigheter, exempelvis riktlinjer kring hur behörighetsadministration i form av tillägg/ändring/borttag av behörigheter skall ske. Vidare saknades riktlinjer gällande krav kring periodiska uppföljningar av behörigheter.

Slutligen saknas en rutinbeskrivning för Falkenbergs kommuns hantering av superusers/administratörs-konton. Aktiviteter i systemen loggas, däremot så finns det ingen rutin på plats för att identifiera och följa upp aktiviteter av superusers/administratörs-konton.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande behörighetshantering då kommunen har en formaliserad rutin för tilldelning, ändring och borttag av behörigheter för nätverk och filstruktur.

Vid granskningen noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi dock Falkenbergs kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.5 i appendix.

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

Falkenbergs kommun använder sig av standardsystem, inga egenutvecklade system finns i verksamheterna. Vidare så hanteras förändringar som görs i verksamhetssystemen på verksamhetsnivå där förvaltningen själva sätter upp en rutin för hur detta skall ske och kontrolleras. Evry ansvarar för att släppa in leverantörer som utför uppdateringarna på aktuell server.

Vid granskningstillfället noterades det att inga rutinbeskrivningar eller riktlinjer är upprättade på övergripande nivå för att stötta nämnderna gällande grundkrav för förändringshantering av system (programförändringar) och det finns inte några kommunicerade krav på kontrollpunkter som bör inkluderas i förändringshantering. Baserat på intervju med utvald nämnd så noterades det att dokumentation och testning av genomförda förändringar genomförs, dock så sparas inte alltid underlag för genomförd testning och gjorda godkännanden.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande hantering av programförändringar då kommunen i stor utsträckning använder sig av standardsystem utan större anpassningar.

Vid granskningstillfället noterades inga iakttagelser som bedöms som hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi dock Falkenbergs kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.6 i appendix.

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

Falkenbergs kommuns primära datahall har bland annat inpasseringsskydd, inbrottslarm, temperatur- och fuktövervakning och kylaggregat. Servrar är upphöjda med rack från golvet (skyddas mot vattenskador) och hallen är utrustad med vattenlarm. Vidare är larm kopplat till upphandlad larmfirma. Korskopplingsrum finns med samma förutsättningar som för datahallen. Slutligen finns UPS som klarar 45 minuter och dieselaggregat som klarar fortsatt drift.

Vid granskningstillfället noterades det att Falkenbergs kommun inte har någon formaliserad rutin gällande kommunens hantering av fysiska behörigheter/passerkort. Det enda som kontrolleras i nuvarande rutin är tillägg av behörigheter, där det görs en rimlighetsbedömning vilken behörighet personen ska ha. Det görs ingen uppföljning att behörigheter är uppdaterade över tid, eller att behörigheter tas bort efter det att personer slutat.

Bedömning

Vår bedömning är att 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 granskningstillfället noterades inga iakttagelser som bedöms som medel eller hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi dock Falkenbergs kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.7 i appendix.

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

Respektive verksamhet ansvarar för avtal mot leverantörer för exempelvis verksamhetssystem. Upphandling för kommungemensamma system är delegerat till respektive enhet som är ansvariga för det specifika systemet, däremot har kommunen nyligen anställt en avtalscontroller (fokusområde avtal och avtalstrohet) som har börjat arbeta med samordningen av befintliga avtal.

Vidare har Falkenbergs kommun valt att outsourca större delen av IT-verksamheten till Evry. Vid granskningstillfället noterades det att kommunen har regelbundna möten med Evry för uppföljning av exempelvis incidenter och problemhantering. Det saknas dock formaliserad uppföljning gällande efterlevnad av avtal relaterat till kritiska områden såsom exempelvis test av avbrottsplan, återläsningstester av backuper, efterlevnad av processer för behörighetshantering och förändringshantering.

Bedömning

Vår bedömning är att kommunen i nuläget ej har en tillräcklig nivå gällande outsourcing och upphandlingar kopplat till IT då kommunen saknar formaliserad uppföljning med Evry gällande efterlevnad av avtal relaterat till kritiska områden såsom exempelvis test av avbrottsplan, återläsningstester av backuper, efterlevnad av processer för behörighetshantering och förändringshantering.

Vi rekommenderar Falkenbergs kommun att utvärdera vilka kontrollpunkter som skall följas upp med viss periodicitet med Evry i komplement till nuvarande driftsmöten. Exempelvis bör uppföljningen inkludera genomförda tester av avbrottsplan, återläsningstester av backuper, efterlevnad av behörighetshanteringskontroller och förändrings-hanteringskontroller.

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

Som redan nämnts i område 3.1 och 3.2 så saknar Falkenbergs kommun detaljerade riktlinjer som säkerställer att IT- och informationssäkerhet hanteras på ett ändamålsenligt sätt i nämnderna. Kommunen har dessutom inte uppdaterat relevanta policydokument, såsom IT-strategi och Informationssäker-hetspolicy, på 8-18 år och saknar en rutin som säkerställer att dessa policydokument regelbundet ses över och uppdateras för att återspegla kommunens verksamhet.

Vidare noterades det även att Falkenbergs kommun har i nuläget ingen uppföljning av efterlevnad av policys och riktlinjer. Kommunen har inte något framtaget ramverk för kontroller inom IT-processer som skall efterlevas av nämnderna (kontrollramverk för generella IT-kontroller) och därmed finns inte heller någon central uppföljning som säkerställer att implementeringen av intern kontroll har gjorts på ett enhetligt och ändamålsenligt sätt.

Sammantaget resulterar detta i att nämnder har en begränsad möjlighet att faktiskt säkerställa att de arbetar med IT- och informationssäkerhet på ett ändamålsenligt sätt.

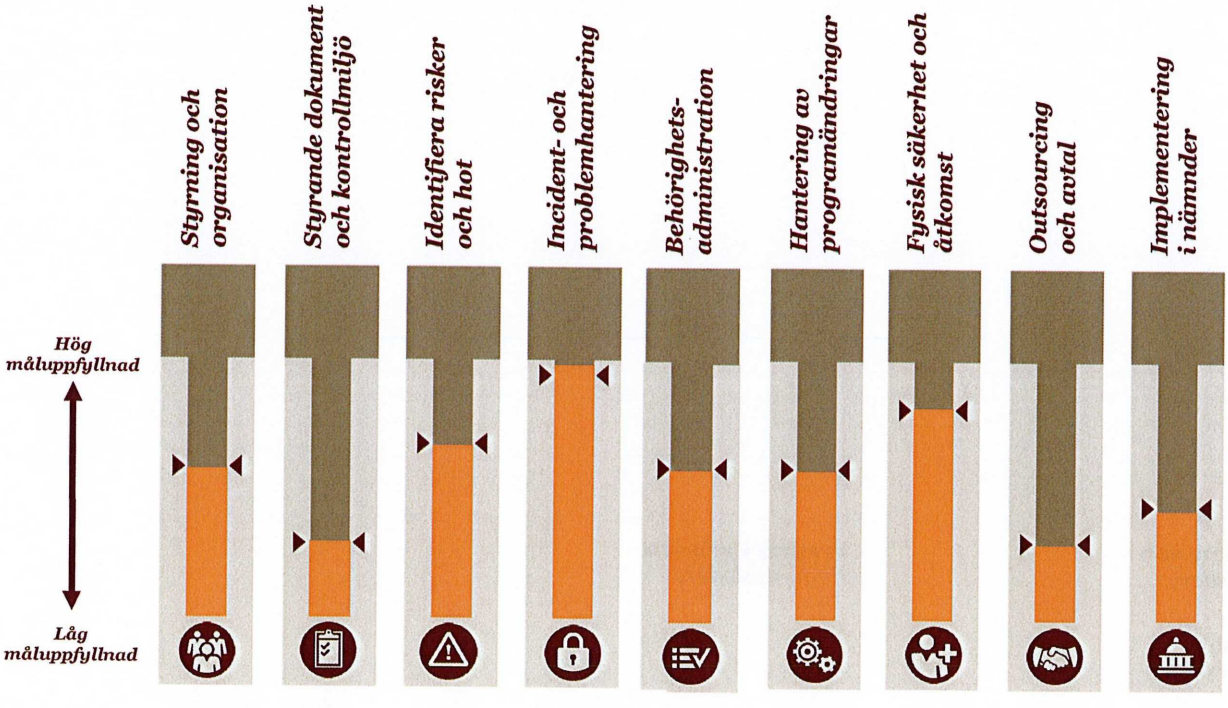
Bedömning

Vår bedömning är att kommunen ej har en tillräcklig nivå gällande krav på nämndernas styrande dokument då det råder en viss otydlighet kring vilka krav som skall uppfyllas för att nämnderna ska nå en ändamålsenlig hantering av IT- och informationssäkerhet.

Vid granskningen noterades iakttagelser som bedöms som både medel och hög risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi Falkenbergs kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.1 – 3.2 i appendix.

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:

Kajsa Jansson
Projektledare

Julia Lahti
Projektmedlem

Fredrik Carlsson
Uppdragsledare

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	*M*	*Falkenbergs kommun har en decentraliserad organisation för systemförvaltning. Detaljerade riktlinjer som säkerställer att IT- och informationssäkerhet hanteras på ett ändamålsenligt sätt i nämnderna finns i nuläget inte framtagna och kommunicerade.*	*Utan tydligt definierade och kommunicerade riktlinjer avseende roller och ansvar kring informationssäkerhet finns det en risk att systemförvaltningen inte styrs på ett effektivt sätt, exempelvis att väsentliga beslut ej tas av korrekt person eller att informationssäkerhetsfrågor inte hanteras i den utsträckning som krävs.*	*Vi rekommenderar att Falkenbergs kommun detaljerar instruktioner för systemförvaltning, exempelvis kring riskanalys, roller och ansvar samt informationssäkerhet, och säkerställer att kommunikation och utbildning sker med berörda.*
3.2	H	Vid granskningstillfället så noterades det att relevanta policydokument, såsom IT-strategi och Informationssäkerhetspolicy, inte uppdaterats på 8-18 år. Vidare saknas en rutin som säkerställer att dessa policydokument regelbundet ses över och uppdateras för att återspegla kommunens verksamhet.	Att policydokument ej uppdateras baserat på förändrad omvärld och förändrade behov försvårar styrningen av verksamheten. Detta kan leda till onödiga kostnader genom att sämre grundade beslut av IT-investeringar och resursallokering sker.	Vi rekommenderar Falkenbergs kommun att se över och uppdatera nuvarande policydokument för att säkerställa att dessa är aktuella och återspeglar kommunens verksamhet, samt införa rutiner där styrdokument ses över och uppdateras regelbundet, förslagsvis en gång per år.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	M	Falkenbergs kommun har i nuläget ingen uppföljning av nämndernas efterlevnad av policys och riktlinjer kopplat till IT. Kommunen har inte något framtaget ramverk för kontroller inom IT-processer som skall efterlevas av nämnderna (kontrollramverk för generella IT-kontroller) och därmed finns inte heller någon central uppföljning som säkerställer att implementeringen av intern kontroll inom detta område har gjorts på ett enhetligt och ändamålsenligt sätt.	Utan uppföljning av efterlevnad av policys och intern kontroll kopplat till IT ökar risken för att dessa policys och instruktioner inte är korrekt implementerade och efterlevs i tänkt utsträckning. Avsaknad av central uppföljning av intern kontrollarbete kopplat till IT ökar risken för att implementerade rutiner och kontroller inte lever upp till kommunens behov (exempelvis informationssäkerhetskrav), samt ökar risken för att IT-kontroller inte är implementerade på ett ändamålsenligt sätt.	Vi rekommenderar Falkenbergs kommun att definiera de grundkrav för intern kontroll inom IT som skall gälla och att implementera rutiner för att centralt följa upp efterlevnad av policys och rutiner kopplat till IT inom nämnderna. Vidare bör IT-organisationen fungera som stöd och en rådgivande funktion gentemot nämnderna för att säkerställa att implementering av intern kontroller kopplat till IT och informationssäkerhet görs på ett enhetligt och ändamålsenligt sätt.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	M	Falkenbergs kommun saknar riktlinjer och instruktioner för genomförande av riskanalyser samt identifiering av kritiska processer och system, så att detta sker på ett likformigt och ändamålsenligt sätt i nämnderna. Verksamheten har inte definierat vilka krav för systemens tillgänglighet (exempelvis upptid och återläsningskrav baserat på genomförda riskanalyser) som skall gälla. Leverantör Evry hanterar avbrottsplan, säkerhetskopiering och återläsningstest, dock är frekvenserna för detta inte kommunicerat och förankrat med verksamheten.	Avsaknad av tydliga instruktioner till hur arbetet med verksamhetsspecifika riskanalyser skall göras kan innebära att verksamheten inte identifierar eller prioriterar sina risker korrekt. Om avbrottsplanen inte bygger på verksamhetens prioriteringar av kritiska system, eller att återläsningsmöjligheter inte uppfyller verksamheten krav, kan det resultera i att resurser sätts till ej tänkta aktiviteter.	Vi rekommenderar Falkenbergs kommun att upprätta riktlinjer och instruktioner som säkerställer att klassificering av kritiska processer/system sker på ett likformigt och ändamålsenligt sätt. Dessa riktlinjer bör även omfatta information om hur systemspecifika återläsningskrav tas fram och hur dessa sedan ska beaktas i säkerhetskopieringspolicy och kontinuitetsplaner. Slutligen bör riktlinjer även omfatta test av avbrotts- och kontinuitetsplaner.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.5	M	Vid granskningstillfället noterades det att inga rutinbeskrivningar eller riktlinjer är upprättade på övergripande nivå för att stötta nämnderna gällande grundkrav för hantering av behörigheter, exempelvis riktlinjer kring hur behörighetsadministration i form av tillägg/ändring/borttag av behörigheter skall. Vidare saknades riktlinjer gällande krav kring periodiska uppföljningar av behörigheter.	Att inte ha en formaliserade krav för rutiner 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 Falkenbergs kommuns IT-system och information.	Vi rekommenderar Falkenbergs kommun att införa en formaliserad rutin för behörighetshantering. Rutinen bör säkerställa att nya, ändrade eller borttagande av behörigheter baseras på en formell ansökan som är attesterad av närmaste chef och/eller systemägare. Slutligen bör rutin även inkludera periodiska genomgångar av befintliga behörigheter för att säkerställa att behörigheter är uppdaterade över tid. Rutinbeskrivningen bör delas med både IT-personal och systemansvariga för verksamhetssystem för att säkerställa att rutinerna implementeras för samtliga system i verksamheterna på ett likvärdigt sätt.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.5	L	Vid granskningen noterades det att kommunen inte gör någon periodisk genomgång av lösenordssättningar för att säkerställa att de förblir enligt kommunens krav över tid.	Felaktigt satta lösenordssättningar, eller lösenordssättningar som inte är i enlighet med kommunens krav, ökar risken för att obehöriga kan ta sig in i kritiska system eller applikationer.	Vi rekommenderar Falkenbergs kommun att implementera rutin för periodisk genomgång av lösenordssättningar för att säkerställa att lösenordssättningar förblir enligt kommunens krav över tid.
3.5	M	Vid granskningstillfället noterades det att det inte fanns någon rutinbeskrivning för Falkenbergs kommuns hantering av superusers/administratörs-konton. Aktiviteter i systemen loggas, däremot så finns det ingen rutin på plats för att identifiera och följa upp aktiviteter av superusers/administratörs-konton.	Avsaknad av rutiner kring uppföljning av loggar kan medföra att felaktigheter och obehörig åtkomst inte upptäcks i tid, alternativt inte upptäcks alls. Vidare kan otillåtna eller felaktiga ändringar i masterdata, exempelvis bankkontonummer, ge påverkan på finansiella transaktioner och riktigheten i den finansiella rapporteringen.	Vi rekommenderar Falkenbergs kommun att se över nuvarande superusers/administratörskonton. Vidare bör kommunen införa en formaliserad rutin för behörighetshantering kopplat till dessa typer av konton och detaljera vilken uppföljning som bör ske av loggade aktiviteter, samt definiera vem som ansvarar för denna uppföljning.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.6	M	Vid granskningstillfället noterades det att inga rutinbeskrivningar eller riktlinjer är upprättade på övergripande nivå för att stötta nämnderna gällande grundkrav för förändringshantering av system (programförändringar) och det finns inte några kommunicerade krav på kontrollpunkter som bör inkluderas i förändringshantering. Baserat på intervju med utvald nämnd så noterades det att dokumentation och testning av genomförda förändringar genomförs, dock så sparas inte alltid underlag för genomförd testning och godkännanden.	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 Falkenbergs kommun att införa en formell ändringsrutin och säkerställa att denna implementeras för drift (IT), kommungemensamma system samt verksamhetssystem. Ändringsrutinen bör innehålla åtminstone: • Riskbedömning av ändringen • 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 kommunen 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
3.7	L	Vid granskningstillfället noterades det att Falkenbergs kommun inte har någon formaliserad rutin gällande kommunens hantering av fysiska behörigheter/passerkort. Det enda som kontrolleras i nuvarande rutin är tillägg av behörigheter, där det görs en rimlighetsbedömning vilken behörighet personen ska ha. Det görs ingen uppföljning att behörigheter är uppdaterade över tid, eller att behörigheter tas bort efter det att personer slutat.	Att inte ha en formaliserad rutin för hantering av fysiska behörigheter/passerkort kan medföra att behörigheter till områden eller lokaler tilldelas en person där denna ej bör ha tillgång. Det kan även innebära att eventuella förändringar av behörigheter blir felaktiga samt att behörigheter som skall tas bort ligger kvar onödigt länge.	Vi rekommenderar Falkenbergs kommun att införa en formaliserad rutin för hantering av fysiska behörigheter/passerkort. Vidare bör kommunen även implementera formaliserade rutiner för periodisk genomgång av tilldelade fysiska behörigheter/passerkort för att säkerställa att dessa är aktuella över tid.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.8	H	Vid granskningstillfället noterades det att kommunen har regelbundna möten med Evry för uppföljning av exempelvis incidenter och problemhantering. Det saknas dock formaliserad uppföljning gällande efterlevnad av avtal relaterat till kritiska områden såsom exempelvis test av avbrottsplan, återläsningstester av backuper, efterlevnad av processer för behörighetshantering och förändringshantering.	Avsaknad av formell uppföljning relaterat till dessa områden ökar risken för att Evry inte lever upp till krav i avtal vilket kan resultera i att kritiska områden för kommunen inte hanteras på ett ändamålsenligt sätt, samt att detta inte identifieras förrän en incident kopplat till detta sker.	Vi rekommenderar Falkenbergs kommun att utvärdera vilka kontrollpunkter som skall följas upp med viss periodicitet med Evry. Exempelvis bör uppföljningen inkludera genomförda tester av avbrottsplan, återläsningstester av backuper, efterlevnad av behörighetshanteringskontroller och förändringshanterings-kontroller.