www.pwc.se

Granskning av IT- och informationssäkerhet

Bollebygds kommun

Januari 2018

Kajsa Jansson
Julia Lahti

Januari 2018

pwc

Innehåll

1. Sammanfattning

De förtroende valda revisorerna i Bollebygds 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 Bollebygds 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 Bollebygds kommun att upprätta instruktioner och rutinbeskrivningar för IT-organisationen för att säkerställa att nuvarande kompetens i IT-organisationen kan tillvaratas av andra personer än enbart nuvarande nyckelpersoner.
- PwC rekommenderar Bollebygds kommun att upprätta en avbrottsplan avseende IT och systemstöd. Kommunen bör dokumentera åtgärder som behöver vidtas, i vilken ordning och av vem, för att effektivt återställa system och applikationer vid en eventuell incident. Baserat på verksamhetens riskanalyser bör kritiska system definieras och få en tydlig prioritering i avbrottsplanen. Vidare bör ansvarsområden beskrivas och kommuniceras till alla berörda, exempelvis genom träning samt testning av planen.
- PwC rekommenderar Bollebygds 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..
- För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi även Bollebygds 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 Bollebygds 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 standader 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:

- Peter Callsen (Administrativ chef och Kommunjurist)
- Klas Höglund (IT-ansvarig och IT-strateg)
- Marco Campopiano (IT-koordinator)
- Christina Hultén (Säkerhetssamordnare)
- Peter Häggquist (Systemförvaltare Raindance)

Granskningen har genomförts under januari 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

Bollebygds kommun har en central organisation för IT, samt i tillägg till detta även en IKT-pedagog vars fokus ligger på skolornas IT-miljö. Kommunen har även utpekade systemförvaltningsroller för samtliga system. Roller och ansvar för dessa personer finns, på en övergripande nivå, beskrivet i Informationssäkerhetspolicy.

Vid granskningen noterades att IT-organisationen i mångt och mycket saknar instruktioner och rutinbeskrivningar, vilket i sin tur resulterat i att det finns ett högt beroende av nyckelpersoner i Bollebygds kommuns IT-organisation.

Bedömning

Vår bedömning är att kommunen i nuläget ej har en tillräcklig nivå gällande styrning av informations- och IT-säkerhet då det råder ett högt personberoende i Bollebygds kommuns IT-organisation.

Vi rekommenderar Bollebygds kommun att upprätta instruktioner och rutinbeskrivningar för IT-organisationen för att säkerställa att nuvarande kompetens i IT-organisationen kan tillvaratas av andra personer än enbart nuvarande nyckelpersoner.

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

Bollebygds kommun har ett antal styrande dokument, såsom IT-strategi, Informationssäkerhetspolicy samt en strategisk plan för informationssäkerhet som beskriver hur kommunen vill arbeta med området informationssäkerhet de kommande åren.

Vid granskningstillfället noterades det däremot att relevanta policydokument, såsom IT-strategi och Informations-säkerhetspolicy, inte uppdaterats på 3-6 år. Vidare saknas en formaliserad rutin som säkerställer att policydokument regelbundet ses över och uppdateras, eller rutin gällande uppföljning av efterlevnad av policys.

Bollebygds kommun har inte något framtaget ramverk för kontroller som bör finnas på plats kopplat till IT-processer (exempelvis godkännande av användare eller uppföljning av genomförda förändringar) utan dessa processer är i nuläget informella.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande styrande dokument då flertal styrande dokument finns framtagna. Trots att dessa inte är uppdaterade så bedöms de fortfarande som relevanta och i mångt och mycket återspeglar dessa Bollebygds kommuns verksamhet.

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 Bollebygds kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.2 i appendix.

3. Resultat av granskningen

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

Iakttagelser

Bollebygds kommun har genomfört en risk- och sårbarhetsanalys och använder sig vidare av Klassa där kritiska system analyseras med fokus på informations-säkerhetskrav. Krav för systemens tillgänglighet (exempelvis upptid och återläsningskrav) har börjat definieras, däremot är detta inte helt färdigställt. För samhällsviktiga system har egna krisplaner, inklusive manuella rutiner/checklistor, tagits fram och som ska tillämpas vid eventuella systemavbrott (kontinuitetsplanering).

Vid granskningstillfället noterades det att det i nuläget inte finns någon aktuell och dokumenterad avbrottsplan (Disaster Recovery Plan - DRP) att tillämpa vid ett eventuellt avbrott avseende IT och systemstöd.

Bedömning

Vår bedömning är att kommunen i nuläget ej har en tillräcklig nivå gällande rutiner för att identifiera och hantera risker och hot då kommunen inte har någon dokumenterad avbrottsplan avseende IT och systemstöd.

Vi rekommenderar Bollebygds kommun att upprätta en avbrottsplan avseende IT och systemstöd. Kommunen bör dokumentera åtgärder som behöver vidtas, i vilken ordning och av vem, för att effektivt återställa system och applikationer vid en eventuell incident. Baserat på verksamhetens riskanalyser bör kritiska system definieras och få en tydlig prioritering i avbrottsplanen. Vidare bör ansvarsområden beskrivas och kommuniceras till alla berörda, exempelvis genom träning samt testning av planen.

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

Bollebygds kommun använder sig av ärendehanterings-systemet Service Manager för rapportering och hantering av incidenter och problem. Det finns en upparbetad rutin för incident- och problemhantering, däremot är denna rutin inte formaliserad i form av dokumentation.

Vid granskningstillfället noterades det att kommunen saknar dokumenterade riktlinjer som säkerställer att prioritering, hantering och uppföljning av incidenter och problem hanteras av utförare på ett enhetligt sätt.

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.

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 Bollebygds kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.4 i appendix.

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

Bollebygds kommuns behörighetshantering skiljer sig åt beroende på om det gäller åtkomst till fil- och nätverksstruktur (Active Directory), kommungemensamma system eller verksamhetssystem. IT-organisationen ansvarar endast för fil- och nätverksstruktur. Behörigheter till verksamhetssystemen hanteras inom respektive nämnd av systemförvaltare.

Vid granskningen noterades det att kommunen saknar formaliserad och dokumenterad rutin gällande tillägg, ändring och borttag av behörigheter. Det finns inte heller någon rutin på plats gällande periodiska uppföljningar av tilldelade behörigheter.

Bedömning

Vår bedömning är att kommunen ej har en tillräcklig nivå gällande behörighetshantering då kommunen saknar formella och dokumenterade rutiner gällande behörighetshantering.

Vi rekommenderar Bollebygds 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.

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

Bollebygds kommun har en ambition att använda sig av standardsystem och ej genomföra någon egen utveckling och anpassning av system i större utsträckning. Denna ambition finns även dokumenterad i nuvarande IT-policy.

Vid granskningstillfället noterades det att Bollebygds kommun i nuläget saknar rutinbeskrivningar och riktlinjer gällande förändringshantering av system (program-förändringar) och det finns inte några kommunicerade krav på kontrollpunkter som bör inkluderas i verksamhetens förändringshantering.

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, dock finns inga rutinbeskrivningar för hur eventuella anpassningar skall ske om dessa utförs.

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 Bollebygds 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

Bollebygds kommuns primära datahall har bland annat inpasseringsskydd, inbrottslarm, temperatur- och fukt-övervakning och kylaggregat. Servrar är upphöjda med rack från golvet (för skydd mot vattenskador) och hallen är utrustad med vattendetektor. Vidare är larm kopplat till Securitas, som i sin tur kontaktar IT-organisationen vid intrång eller incidenter. Korskopplingsrum finns med samma förutsättningar som för datahallen.

Vidare finns UPS som med en räckvidd på 45 minuter och dieselaggregat som klarar fortsatt drift. Dieselaggregatet är placerat i en separat närliggande byggnad och testas regelbundet av kommunen.

Slutligen så har uppföljning till inpassering och behörigheter till kommunens driftslokaler gjorts under det senaste året, däremot finns det ingen formaliserad rutin för detta.

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 granskningen noterades inga iakttagelser kopplat till kontrollmålet.

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

Bollebygds kommun har valt att ha en multi-sourcad miljö. Nämnderna ansvarar själva för upphandling av system och IT-tjänster, IT-upphandlingar stöttas av IT-organisationen i den mån upphandlaren väljer att involvera IT. Vidare är det en låg grad av tjänsteavtal, framförallt köper kommunen in produkter och tjänsteprodukter snarare än rena outsourcing-tjänster.

Vid granskningstillfället så noterades att samtliga avtal kopplat till system och IT inte finns samlat i avtalsdatabas för uppföljning och överblickbarhet (exempelvis kring avtalens löptider).

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande outsourcing och upphandlingar kopplat till IT.

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 Bollebygds kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.8 i appendix.

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 nämnts i område 3.1 och 3.2 så finns det ett högt personberoende i Bollebygds kommuns IT-organisation. IT-organisationen saknar i mångt och mycket instruktioner och rutinbeskrivningar. Systemförvaltningsroller finns definierade men det finns inga detaljerade och väl kommunicerade rollbeskrivningar som säkerställer en god nivå av informationssäkerhet. Slutligen så har relevanta policydokument, såsom IT-strategi och Informations-säkerhetspolicy, inte uppdaterats på 3-6 år, och det görs ingen uppföljning av efterlevnad av policys och eventuella avsteg från dessa som nämnderna väljer att göra.

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

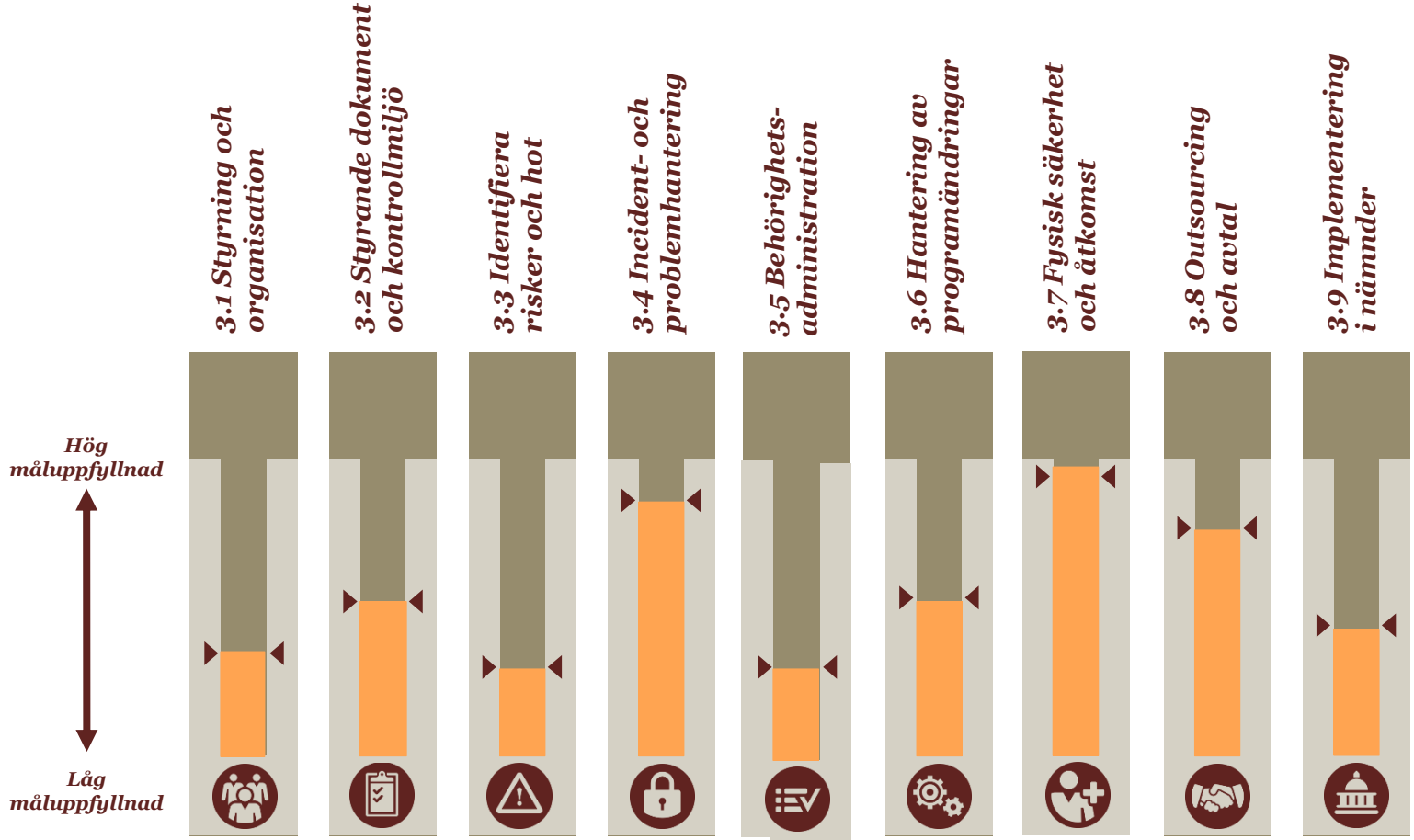
Bedömning

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.

För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi Bollebygds 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	Vid granskningstillfället noterades det att Bollebygds kommun har utpekade systemförvaltningsroller för samtliga system. Roller och ansvar för dessa personer finns övergripande beskrivet i Informationssäkerhetspolicy, dock bör detaljerade rollbeskrivningar tas fram och kommuniceras ut för att säkerställa en god nivå av informationssäkerhet.	Utan tydligt definierade och kommunicerade roller 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 Bollebygds kommun detaljerar roller och ansvar för systemförvaltningsroller samt säkerställer att kommunikation och utbildning sker till alla berörda.
3.1	H	Det finns ett högt beroende av nyckelpersoner i Bollebygds kommuns IT-organisation. Detta på grund av att IT-organisationen i mångt och mycket saknar instruktioner och rutinbeskrivningar.	Ett högt personberoende av nyckelpersoner ökar risken för att kompetens försvinner om nyckelperson väljer att sluta eller av annan anledning inte finns tillgänglig, vilket i sin tur ökar risken för att väsentliga arbetsmoment inte utförs på ett ändamålsenligt sätt.	Vi rekommenderar Bollebygds kommun att upprätta instruktioner och rutinbeskrivningar inom väsentliga områden 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
3.2	M	Vid granskningstillfället så noterades det att relevanta policydokument, såsom IT-strategi och Informationssäker-hetspolicy, inte uppdaterats på 3-6 år trots att kommunen har ändrade förhållnings- och arbetssätt till IT- och informationssäkerhet. Vidare saknas en rutin som säkerställer att dessa policydokument regelbundet ses över och uppdateras.	Att policydokument ej uppdateras baserat på förändrad omvärld och förändrade behov försvårar styrningen av verksamheten och kan leda till onödiga kostnader genom sämre grundade beslut av IT-investeringar och resursallokering sker.	Vi rekommenderar Bollebygds 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.
3.2	M	Bollebygds kommun har i nuläget ingen uppföljning av efterlevnad av policys. Det finns heller inte något framtaget ramverk för kontroller som bör finnas på plats kopplat till IT-processer (exempelvis godkännande av användare eller uppföljning av genomförda förändringar).	Utan uppföljning av efterlevnad av policys ökar risken för att policys inte är korrekt implementerade och efterlevs i tänkt utsträckning. Utan ett formellt kontroll-ramverk finns risken att implementerade rutiner och kontroller inte lever upp till kommunens behov (exempelvis informationssäkerhetskrav).	Vi rekommenderar Bollebygds kommun 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 uppföljning av efterlevnad av kontroller och policys.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	L	Eftersom en samlingsplan är ett krav enligt BFNAR 2013:2, bör samtliga kritiska system ha en samlingsplan upprättad. Bollebygds kommun har inventerat vilka system som har en samplingsplan ("logisk skiss systemsamband"), dock så finns det ingen uppföljning där kommunen säkerställer att alla kritiska system har en samlingsplan upprättad.	En svagt dokumenterad IT-miljö och dess behörigheter innebär ökade risker vid personal-omsättning samt kan innebära onödiga extrakostnader vid inköp av nya system och applikationer. Vidare kan en bristfällig förståelse för IT-miljöns sammansättning öka risken för störningar i IT systemen vid uppgraderingar.	Vi rekommenderar Bollebygds kommun att följa upp den inventeringen som gjorts för att säkerställa att samtliga kritiska system har en samlingsplan. Översiktligt bör samplingsplanen beskriva nätverk och IT-miljö (t ex nätverkskarta), hårdvara, mjukvara, informationsflöde samt övrig relevant information som krävs för att få en god förståelse för befintlig struktur. Vidare kan driftrutiner etc. med fördel kopplas ihop med denna information.
3.3	M	Kommunens verksamheter har i samband med informationssäkerhetsanalys påbörjat att definiera vilka krav för systemens tillgänglighet (exempelvis upptid och återläsningskrav) som skall gälla. Detta bör dock sedan tas vidare till IT för att skapa en dokumenterad säkerhets-kopieringspolicy som möter dessa krav.	Avsaknad av tydliga krav, samt avsaknad kring återkoppling på att dessa krav uppfylls för kommunens system, kan innebära en risk att tillgänglighet och återläsningsmöjligheter inte uppfyller verksamheten krav.	Vi rekommenderar Bollebygds kommun 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 och återspeglas i säkerhetskopieringspolicy.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	H	Bollebygds kommun har i nuläget inte någon formellt dokumenterad avbrottsplan (Disaster Recovery Plan - DRP) att tillämpa vid ett eventuellt avbrott avseende IT och systemstöd.	Avsaknad av dokumenterade planer medför i 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. Det kan även innebära att resurser sätts till ej tänkta aktiviteter om avbrottsplanen inte bygger på verksamhetens prioriteringar av kritiska system.	Vi rekommenderar Bollebygds kommun att dokumentera åtgärder som behöver vidtas, i vilken ordning och av vem, för att effektivt återställa system och applikationer vid en eventuell incident. Baserat på verksamhetens riskanalyser bör kritiska system definieras och få en tydlig prioritering i avbrottsplanen. Vidare bör ansvarsområden beskrivas och kommuniceras till alla berörda, exempelvis genom träning samt testning av planen.
3.4	L	Vid granskningstillfället noterades det att det inte återfinns någon rutinbeskrivning för incident- och problemhantering som säkerställer att uppföljning sker på samma sätt av alla utförare. Detta resulterar också i att det finns en ökad risk för högt personberoende i processen.	Utan rutiner för uppföljning av incidenter så finns det en risk för att monitorering och uppföljning av incidenter inte sker på samma sätt av samtliga utförare och ökar risken för att problem ej upptäcks eller säkerställs för fullständig hantering. Det kan också innebära att mönster kring upprepade incidenter inte upptäcks och analyseras.	Vi rekommenderar Bollebygds kommun att ta fram en rutin för hur incidenter ska följas upp och säkerställa att denna är kommunicerad till samtliga utförare.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.5	H	Vid granskningstillfället så fanns inga rutinbeskrivningar upprättade för Bollebygds kommuns hantering av behörigheter, exempelvis saknas dokumenterade rutiner för behörighetsadministration i form av tillägg/ändring/borttag av behörigheter men även periodiska uppföljningar av behörigheter.	Att inte ha en formaliserad 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 Bollebygds kommuns IT-system och information.	Vi rekommenderar Bollebygds 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.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.5	L 	Vid granskningen noterades det att kommunen har låga lösenordskrav på exempelvis tid för lösenordens giltighet i jämförelse med god praxis. Vidare görs ingen periodisk genomgång av lösenordssättningar för att säkerställa att de förblir enligt kommunens krav över tid.	Låga lösenordskrav ökar risken för att obehöriga kan ta sig in i kritiska system eller applikationer, särskilt vid tillämpning av Single Sign On.	Vi rekommenderar att Bollebygds kommun att utvärdera om lösenordskraven är tillräckliga i förhållande till informationssäkerhetskrav, speciellt vid en framtida tillämpning av Single Sign On.
3.5	M 	Vid granskningstillfället noterades det att det inte fanns någon rutinbeskrivning för Bollebygds kommuns hantering av superusers/administratörskonton, eller riktlinjer gällande hantering av behörigheter till konsulter. Aktiviteter i systemen loggas, däremot så finns det ingen rutin på plats för att identifiera och följa upp aktiviteter av superusers/administratörskonton.	Att inte ha en formaliserad rutin för hantering av superusers/administratörskonton, eller hantering av behörigheter till konsulter, kan medföra att behörigheter tilldelas till personal som inte skall ha tillgång till en specifik resurs eller tjänst. Detta kan påverka säkerheten för Bollebygds kommuns IT-system och information.	Vi rekommenderar Bollebygds kommun att se över nuvarande superusers/administratörskonton och konsulters behörigheter, samt att införa en formaliserad rutin för behörighetshantering kopplat till dessa typer av konton och vilken uppföljning som bör ske av loggade aktiviteter. Rutinen bör säkerställa att superusers/administratörskonton är begränsat till ett lämpligt antal och relevanta medarbetare, samt att behörigheter till konsulter är personliga och inte löper utanför konsultens arbetstid och aktiviteter hos kommunen.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.6	M	Vid granskningstillfället noterades det att det inte fanns någon rutinbeskrivning 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. Detta kan i slutändan påverka system och applikationers riktighet, sekretess och tillgänglighet.	Vi rekommenderar Bollebygds 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
3.8	M	Vid granskningstillfället så noterades att samtliga avtal kopplat till system och IT inte finns samlat i avtalsdatabas för uppföljning och överblickbarhet (exempelvis kring avtalens löptider).	Utan en samlad bild över samtliga avtal finns risk för att avtal löper ut eller överträds utan att detta upptäcks av kommunen.	Vi rekommenderar Bollebygds kommun att säkerställa att samtliga avtal för system och IT samlas i avtalsdatabas för enklare inventering och uppföljning.