www.pwc.se

Granskning av IT- och informationssäkerhet

Marks kommun

December 2017

Kajsa Jansson
Vilhelm Kokko

December 2017

pwc

Innehåll

1. Sammanfattning

De förtroende valda revisorerna i Marks 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 Marks 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 att aktuella policy-dokument tas fram och formellt godkännas. Dessa skall återspegla dagens förutsättningar och blicka framåt. Vikt bör läggas på att kommunicera och förankra innehållet samt att hålla det levande över tiden.
- PwC rekommenderar Marks kommun att fortsätta arbetet med att utveckla den förvaltningsmodell som började tas fram under 2014. En förvaltningsmodell bör innehålla områdena förvaltningsstyrning, användarstöd, ändringshantering och drift och underhåll.
- PwC rekommenderar att Marks kommun utför en mer omfattande risk och sårbarhetsanalys där befintliga IT-system och relaterade risker utvärderas. En riskanalys som täcker in flertalet IT-relaterade risker gör kommunen bättre förberett vid en eventuell incident och kan ge indikationer på var åtgärder för att stärka kontroller och rutiner kan behövas. Som en del i detta bör information klassificeras baserat på konfidentialitet, riktighet och tillgänglighet.
- PwC rekommenderar Marks kommun 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.
- PwC rekommenderar Marks kommun att införa en formaliserad rutin för hantering av behörigheter vilken bör kommuniceras som krav för samtliga system, kommungemensamma såväl som verksamhetssystem. Rutinen bör bygga på att en formell ansökan om behörighet skickas till IT-avdelningen.
- För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi även Marks 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 Marks 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 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.

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:

Marks kommun IT:
- Krister Näsström (IT-chef)
- Jonas Emanuelson (Systemtekniker)
- Tomas Szigeti (Systemtekniker)

Granskningen har genomförts under december 2017 av Kajsa Jansson (projektledare) och Vilhelm Kokko, 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

Marks kommun har en central organisation för IT med framförallt en IT-avdelning för kommunen och ett fåtal resurser ute i nämndernas verksamhet, framförallt kopplat till Utbildningsnämnden.

I granskningen har vi dock noterat att Marks kommun i nuläget saknar en formellt utsedd informationssäkerhetsansvarig samt att Marks kommun i nuläget inte har formellt utpekade systemägare för övriga system än de kommungemensamma, och det finns inte heller någon definition som beskriver vad ett kommungemensamt system är. Vidare finns heller ej fullt ut uppdaterade rollbeskrivningar för dessa roller (exempelvis systemägare, systemansvarig).

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande styrning av informations- och IT-säkerhet då kommunens organisation har tydliga funktioner för IT- och 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 Marks 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

Marks kommun har ett antal styrande dokument, exempelvis en IT-policy, som är framtagna under 2013 och godkända av Kommunstyrelsen. Dessa har giltighetstid på 5 år och skall uppdateras 2018.

Vid granskningstillfället så noterades det att inte samtliga policydokument inom kommunen är slutgiltiga, nuvarande dokument hänvisar även till underliggande dokument vilka är arbetsdokument. I nuläget saknas även en formell IT-användarpolicy.

Marks kommun har i nuläget inte någon antagen förvaltningsmodell (ett utkast finns vilket dock inte är antaget eller implementerat i verksamheten). Enligt IT-säkerhetspolicy skall nämnderna implementera egna rutiner för verksamhetsunika system, dock finns det ingen förvaltnings-modell som anger hur detta ska ske eller hur roller och ansvar skall fördelas för detta mellan nämnderna och Marks kommuns IT.

Bedömning

Vår bedömning är att kommunen i nuläget ej har en tillräcklig nivå gällande styrande dokument då ej samtliga policys och rutinbeskrivningar är formellt antagna och en tydlig förvaltningsmodell för kommunens system saknas.

PwC rekommenderar Marks kommun att fortsätta det påbörjade arbetet med genomgång av policys och instruktioner, och att sätta formerna för hur en förvaltningsmodell skall se ur för kommunen. 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 hanteras nya risker och hot?

Iakttagelser

Marks kommun har genomfört ett antal riskanalyser fokuserade mot specifika områden, exempelvis inför upphandling av ny serverpark genomfördes analys över nuvarande och risker och sårbarheter kopplat till detta. Vidare finns ett utkast till förvaltningsmodell framtaget 2014 (dock ej antagen), vilken innehåller exempelvis beskrivning över roller och ansvar, genomförande av informations-säkerhetsklassificering och krav på säkerhetskopiering.

Vid granskningstillfället så noterades det att enligt Marks kommuns IT-säkerhetspolicy skall riskanalyser för informations- och IT-miljö göras, detta har dock inte skett ännu. Vidare finns det ingen informationsklassificering framtagen.

Vidare finns ett utkast till avbrottsplan (Disaster Recovery Plan - DRP) men att denna är i behov av uppdatering och utveckling. Det noterades även att kommunen saknar riktlinjer för hur nämnderna skall ta fram kontinuitetsplaner (Business Continuity Plan – BCP) för manuell hantering vid ett systemavbrott.

Bedömning

Vår bedömning är att kommunen i nuläget ej har en tillräcklig nivå gällande rutiner för att identifiera och hantera risker och hot då en formell riskanalys för IT- och informationsrisker ej genomförts. Som ett nästa steg har därmed inte verksamhetens krav för de olika implementerade systemen definierats.

PwC rekommenderar Marks kommun att utföra en mer omfattande risk och sårbarhetsanalys där befintliga IT-system och relaterade risker utvärderas och prioriteras. En riskanalys som täcker in flertalet IT-relaterade risker gör kommunen bättre förberett vid en eventuell incident och kan ge indikationer på var åtgärder för att stärka kontroller och rutiner kan behövas. Som en del i detta bör information klassificeras baserat på konfidentialitet, riktighet och tillgänglighet.

PwC rekommenderar även Marks kommun att dokumentera de åtgärder som behöver vidtas vid ett avbrott, i vilken ordning och av vem, för att effektivt återställa system och applikationer vid en eventuell incident.

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

Marks kommun har ingen formell rutinbeskrivning för incident- och problemhantering, däremot finns ett satt workflow i Ivanti (ärendehanteringssystem). Uppföljning av incidenter sker av IT-avdelningen som en daglig aktivitet och mätning sker av antal ärenden som ligger upplagda i ärendehanteringssystemet. Marks kommun saknar dock en rutin för kontinuerlig uppföljning av incidenter.

Ett grundläggande skydd för externa intrång finns på plats i form av installerade brandväggar och system för intrångsskydd (Intrusion Prevention System – IPS).

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande incidenthantering då uppsatt workflow i ärendehanteringssystem finns och aktiviteter inom området sker baserat på behov. 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 Marks 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

Marks kommun har en rutin för hur behörighetshantering sker för nätverksstruktur (Active Directory) samt vissa kommungemensamma system. Det finns ingen rutinbeskrivning men ett styrande workflow i ärendehanteringssystemet för dessa typer av behörigheter. Förfrågan av behörigheter sker genom ServicePortal och anställande chef genomför godkännande innan tillägg görs av IT-avdelningen. Marks kommun har även ett pågående projekt för att koppla ihop Active Directory med personalsystem (för automatisk skapande och borttagning av AD-behörighet).

Vid granskningstillfället så fanns ingen generell process beskriven för Marks kommuns hantering av behörigheter, exempelvis behörighetsadministration i form av tillägg/ändring/borttag av behörigheter och uppföljning av behörigheter.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande behörighetshantering för kommungemensamma system då informella rutiner för upplägg och ändring finns på plats. För övriga system så har ingen granskning gjorts, dock finns inga generella riktlinjer som beskriver hur behörighetsadministration bör ske.

PwC rekommenderar Marks kommun att införa en formaliserad rutin för hantering av behörigheter vilken bör kommuniceras som krav för samtliga system, kommungemensamma såväl som verksamhetssystem. Rutinen bör bygga på att en formell ansökan om behörighet skickas till IT avdelningen. Ansökan bör vara undertecknad av närmaste chef och/eller systemägare för den som skall ha behörighet. Detta bör även gälla vid förändring och borttagande av behörigheter.

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

Marks kommun har en ambition att använda sig av standardsystem och ej genomföra större mängder förändringar till standardfunktionalitet. Konsulter har inte ständig behörighet till kommunens system utan måste ges behörighet baserat på specifika uppgifter som skall genomföras.

I granskningen har vi dock noterat att Marks kommun i nuläget saknar rutinbeskrivning för förändringshantering av system (programförändringar) och det finns inte några kommunicerade krav på kontrollpunkter som bör inkluderas i förändringshantering.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande hantering av programförändringar. Informella rutiner för hantering av förändringar finns på plats, dock är dessa inte dokumenterade och för övriga system än kommungemensamma finns inga generella riktlinjer som beskriver hur förändringshantering bör ske. 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 Marks 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

Marks kommun har två datacenter för driften av kommunens IT- och systemmiljö. Den primära datahallen har bland annat inpasseringsskydd, temperatur- och fuktövervakning och skydd mot bortfall i elförsäljning (exempelvis UPS och dieselaggregat). Den sekundära datahallen är en så kallad ”kall site” utan hårdvara eller annan utrustning uppsatt men med förutsättningarna för uppsättning av driftsmiljö. Drift och övervakning sker av IT-avdelningens personal. Marks kommun har initierat ett projekt för att se över framtidens datahallsmiljö och utvärdera de fysiska driftslösningarna.

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 som bedöms som hög eller medium risk. För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi dock Marks 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

Marks kommun har en upphandlingsansvarig för IT som ansvarar för kommungemensamma system. Nämnderna ansvarar själva för upphandling av system och IT-tjänster som är verksamhetsspecifika. Det finns en upphandlingspolicy som antogs 2015 som även omfattar IT-system. Marks kommuns IT-upphandlare håller på att gå igenom samtliga avtal för att säkerställa att alla avtal är giltiga.

Det finns i nuläget ingen samordning mellan IT-inköp, dock är detta en planerad aktivitet för Tjänsteteamet som kommer att ansvara för att inhämta information från förvaltningarna med viss periodicitet och säkerställa att behov och pågående projekt fångas upp och aggregeras.

Bedömning

Vår bedömning är att kommunen 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 vi dock Marks 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

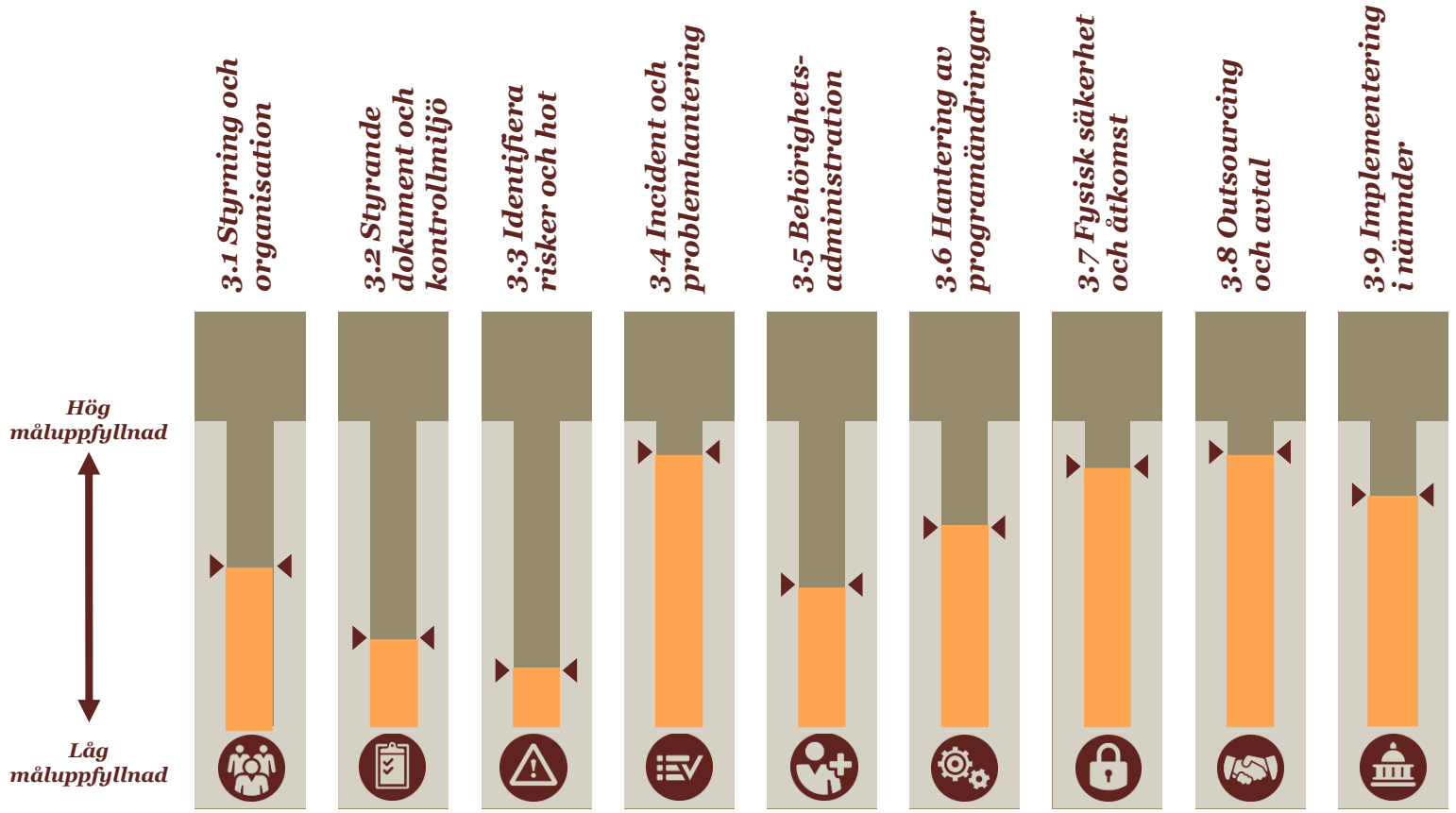
Marks kommun har flertal styrande dokument på kommunövergripande nivå. Vid en genomgång av de styrande dokument så noterade vi att det finns en sektion i IT-säkerhetspolicyn som beskriver att nämnderna skall efterleva kommungemensamma rutiner och ramverk. Dock bör det säkerställas att det är tydligt vilka dessa rutiner och ramverk som åsyftas är.

Bedömning

Vår bedömning är att kommunen har en tillräcklig nivå gällande krav på nämndernas styrande dokument, dock råder viss otydlighet kring mer specifikt vilka krav som skall uppfyllas. 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 Marks kommun att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i område 3.9 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

Fredrik Carlsson
Uppdragsledare

Vilhelm Kokko
Projektmedlem

Appendix: Sammanställning avvikelser

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

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

Prioritet	**Förklaring till prioritet**
Hög	Syftar på en svaghet som har stor inverkan på system, processer och relaterade kontroller och som kan utsätta enheten för större förluster, ineffektivitet och/eller kan resultera i en väsentlig felaktighet i räkenskaperna.
Medel	Syftar på en situation eller arbetssätt som skiljer sig från vad PwC anser vara god praxis och som vi bedömer har en negativ inverkan på den interna kontrollen 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 granskningen noterades det att Marks kommun i nuläget saknar en formellt utsedd informationssäkerhetsansvarig.	För att kunna skapa och bibehålla tillräcklig kontroll över kommunens information och säkerställa välgrundade prioriteringar är det viktigt att utse en person med ett formellt övergripande informationssäkerhetsansvar.	Vi rekommenderar Marks kommun att överväga fördelarna med att ha en formellt ansvarig och uttalad informationssäkerhetsansvarig. Den som är ansvarig för informationssäkerheten kommer att ha en viktig roll i att definiera, bibehålla samt kommunicera de informationssäkerhetskrav som kommunen har.
3.1	M	Marks kommun har i nuläget inga formellt utpekade systemägare för övriga system än de kommungemensamma, och det finns inte heller någon definition som beskriver vad ett kommungemensamt system är. Vidare finns heller ej fullt ut uppdaterade rollbeskrivningar för dessa roller (exempelvis systemägare, systemansvarig).	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 Marks kommun fastställer ansvarsfördelningen av IT-systemen. 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, exempelvis kring att systemägare skall ansvara för att definiera och upprätthålla rätt säkerhetsnivå för respektive system.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	H 	Vid granskningstillfället så noterades det att inte samtliga policydokument inom kommunen är slutgiltiga, nuvarande dokument hänvisar även till underliggande dokument vilka är arbetsdokument. I nuläget saknas även en formell IT-användarpolicy.	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.	Aktuella policy-dokument bör tas fram och formellt godkännas. Dessa skall återspegla dagens förutsättningar och blicka framåt. Vikt bör läggas på att kommunicera och förankra innehållet samt att hålla det levande över tiden.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	H 	Marks kommun har i nuläget inte någon antagen förvaltningsmodell (utkast finns vilket dock inte är antaget eller implementerat). Enligt IT-säkerhetspolicy skall nämnderna implementera egna rutiner för verksamhetsunika system, dock finns det ingen förvaltnings-modell som anger hur detta ska ske eller hur roller och ansvar skall fördelas för detta mellan nämnderna och Marks kommuns IT.	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 Marks kommun att fortsätta arbetet med att utveckla den förvaltningsmodell som började tas fram under 2014. En förvaltningsmodell bör innehålla områdena förvaltningsstyrning, användarstöd, ändringshantering och drift och underhåll, exempelvis: • Definierade roller och ansvar för systemet (samt ansvarsfördelning mellan IT och förvaltningar). • Riskanalys • Systemmiljö • Informationssäkerhetskrav • Systemspecifika rutinbeskrivningar och kontroller • Krav på tillgänglighet och säkerhetskopiering

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.2	M	Marks kommun har i nuläget ingen uppföljning av efterlevnad av policys. Det finns heller inte något framtaget ramverk för intern kontroll gällande IT.	Utan uppföljning av efterlevnad finns det risk 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 Marks 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.
3.3	L	Marks kommun har inte någon eller några framtagna samlingsplan(er) på kommungemensam nivå eller för nämnderna förutom för vissa undantag (ex ekonomisystem), vilket är ett krav enligt BFNAR 2013:2.	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 då uppgraderingar ska genomföras.	En samlingsplan bör tas fram baserat på genomgång av IT-miljön. Översiktligt bör denna beskriva nätverk och IT-miljö (t ex nätverkskarta), hårdvara, mjukvara 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.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	H	Enligt Marks kommuns IT-säkerhetspolicyn skall riskanalyser för informations- och IT-miljö göras, detta har dock inte skett ännu. Vidare finns det ingen informations-klassificering framtagen.	Att inte regelbundet genomföra riskanalyser för verksamheten där risker och hot identifieras kan medföra att risker förbises som kan medföra skada för bolaget.	Vi rekommenderar att Marks kommun utför en mer omfattande risk och sårbarhetsanalys där befintliga IT-system och relaterade risker utvärderas. En riskanalys som täcker in flertalet IT-relaterade risker gör kommunen bättre förberett vid en eventuell incident och kan ge indikationer på var åtgärder för att stärka kontroller och rutiner kan behövas. 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 upptid och återläsningskrav) som skall gälla. IT 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 kommunens system, kan innebära en risk att tillgänglighet och återläsningsmöjligheter inte uppfyller verksamheten krav.	Vi rekommenderar Marks 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.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	H	Vid granskningen noterades att Marks kommun har en avbrottsplan (Disaster Recovery Plan - DRP) men att denna är i behov av uppdatering och utveckling. Det noterades även att kommunen saknar riktlinjer för hur nämnderna skall ta fram kontinuitetsplaner (Business Continuity Plan – BCP) för manuell hantering vid ett systemavbrott.	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 leder även till en ökad risk för att verksamheten blir utan systemstöd längre än nödvändigt samt att verksamheten avstannar helt vid systembortfall.	Vi rekommenderar Marks kommun 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. Katastrof- och kontinuitetsplanerna bör vidare stämmas av med eventuella leverantörer så att de återställningskrav som definierats reflekteras av de servicekontrakt som finns.
3.4	L	Ingen rutinbeskrivning för incident- och problemhantering kunde noteras vid granskningstillfället, däremot finns ett satt workflow i Ivanti (ärendehanteringssystem). Marks kommun saknar dock en rutin för kontinuerlig uppföljning av incidenter.	Utan riktlinjer samt rutiner för uppföljning av incidenter så finns det en risk för att incidenter inte upptäcks eller säkerställs för fullständig hantering. Det kan också innebära att mönster kring upprepade incidenter inte upptäcks och analyser.	Vi rekommenderar Marks kommun att ta fram en rutin för hur incidenter ska följas upp och säkerställa att det finns en utpekad ansvarig för dessa aktiviteter.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.5	H	Vid granskningstillfället så fanns ingen generell process beskriven för Marks kommuns hantering av behörigheter, exempelvis behörighetsadministration i form av tillägg/ändring/borttag av behörigheter och uppföljning 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 Marks kommuns IT-system och information.	PwC rekommenderar Marks kommun att införa en formaliserad rutin för hantering av behörigheter vilken bör kommuniceras som krav för samtliga system, kommungemensamma såväl som verksamhetssystem. Rutinen bör bygga på att en formell ansökan om behörighet skickas till IT avdelningen. Ansökan bör vara undertecknad av närmaste chef och/eller systemägare för den som skall ha behörighet. Detta bör även gälla vid förändring och borttagande av behörigheter.

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 Marks kommun att införa en formell ändringsrutin och kommunicera denna med eventuella berörda 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 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
3.6	L	Patchar hanteras enbart utav en person och utförs baserat på denna persons kunskap (formella rutinbeskrivningen finns ej). Det finns ingen tydlig rutin för uppföljning av hur patcharna läggs på, och det finns inte utpekat vem som ska göra denna uppföljning.	Risken med att inte ha någon tydlig rutin för hur systemen skall patchas är att stor del av kunskapen blir baserad på enskilda individer och det finns en risk för personberoende i vissa processer.	Marks kommun bör implementera en gemensam rutin för hantering av patchar i de olika systemen. Rutinen bör ange lägsta acceptabla patchnivå för de olika systemen, hur patchar skall läggas på samt vilka uppföljningar som skall göras i miljön.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.7	L	Det finns ett utkast till riktlinje för lösenordssättningar framtaget utav IT-chef. Denna är dock ej formellt antagen. Vidare görs ingen periodisk genomgång av lösenordssättningar.	Avsaknad av formellt definierade och implementerade lösenordsparametrar ökar risken för otillåten åtkomst till operativsystemet, vilket ökar risken för obehörig åtkomst till finansiella applikationer.	Vi rekommenderar att kommunen slutför arbetet med att ta fram och implementera en lösenordspolicy samt att säkerställa att regelbundna genomgångar av lösenords-sättningarna för att verifiera att de lösenord som krävs för att gå åtkomst till operativsystem, filer, och program är i linje med den upprättade policyn.
3.7	L	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.	Avsaknad av en formellt kontroll för att fastställa vilka/hur många anställda hos Marks kommun 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 Marks kommun 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 kommunen regelbundet följer upp vilka som har tillgång till serverrum för att se så att rätt personer har åtkomst över tid.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.8	L	Vid granskningstillfället noterade vi att Marks kommun har en god grund kring upphandlingar av IT då det finns både en IT-upphandlare och en upphandlingspolicy. Dock noterade vi att det saknas en samordning mellan IT-inköp.	Det finns en risk för suboptimering om det inte finns en process för hur samordning mellan IT-inköp bör ske.	Vi rekommenderar Marks kommun att utvärdera om det finns ett behov av samordning av IT-inköp, exempelvis genom att fortsätta det påbörjade arbetet med att tjänsteteamen har detta som en del i sina avstämningar med nämnderna.
3.9	M	Vid genomgång av styrande dokument så noterade vi att det finns en sektion i IT-säkerhetspolicyn som beskriver att nämnderna skall efterleva kommungemensamma rutiner och ramverk. Dock bör det säkerställas att det är tydligt vilka dessa rutiner och ramverk som åsyftas är.	Utan formellt definierade krav på nämndernas implementering av policys och rutiner, och godkännande av avsteg från dessa, finns en risk att förväntad nivå på IT-och informationssäkerhet inte finns implementerad.	Vi rekommenderar Marks kommun att säkerställa att det är tydligt vilka krav på IT- och informations-säkerhet som gäller för nämnderna. I detta bör även tydligt ingå vem som kan godkänna avsteg från dessa rutiner och hur denna process sker.