www.pwc.se

Granskning av IT-säkerhet

Mariestads, Törebodas och Gullspångs kommuner

November 2018

Rolf Svärd
Robin Karlsson

November 2018

pwc

Innehåll

1. Sammanfattning

Revisorerna för Mariestads, Törebodas samt Gullspångs kommun (nedan kallade MTG) har gett PwC i uppdrag att genomföra en granskning av IT-säkerhet för att besvara revisionsfrågan:

Är kommunens organisation och interna kontroll ändamålsenlig och tillräcklig när det gäller IT-säkerhet?

Efter genomförd granskning är vår samlade bedömning att IT-säkerheten, ur ett övergripande perspektiv, är delvis ändamålsenlig för att stödja verksamheten och ge tillräcklig intern kontroll. Detta genom att MTG har framtagen dokumentation, lämpliga roller för IT- och informationssäkerhet och även visat en vilja på att åtgärda kvarstående svagheter. Vi har däremot noterat ett antal områden där IT-säkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll inom IT. Flera åtgärder är redan påbörjade av MTG inom dessa områden men behöver slutföras.

Nedan redovisar vi våra mest väsentliga rekommendationer.

- PwC rekommenderar MTG att införa en process för att regelbundet analysera, dokumentera och förankra acceptabel risknivå med IT-nämnden. Detta för att ge underlag till IT-nämnden som har till uppgift att säkerställa en hög kvalitet i verksamheten.
- PwC rekommenderar MTG att upprätta en utbildningsplan för att säkerställa att alla medarbetare kontinuerligt får utbildning inom informationssäkerhet.
- PwC rekommenderar MTG att arbeta fram och implementera ett internt kontrollramverk över relevanta kontroller som utförs i organisationerna kopplat till IT.
- PwC rekommenderar MTG att definiera säkerhetsåtgärder som kopplar till dokument för klassificeringen av information, med ändamålet att skydda information på lämpligt sätt.
- PwC rekommenderar MTG att genomföra en risk- och sårbarhetsanalys kopplad till IT-säkerhet. Samt säkerställa att analysen kontinuerligt följs upp och hålls uppdaterad.
- PwC rekommenderar MTG att fortsätta arbetet med att implementera metod för klassificering av system och dokumentera i styrande dokumentation.
- PwC rekommenderar IT-förvaltningen att ta fram en systemöversikt för att visualisera hela IT-miljön, för att minska risker vid personalomsättning och underlätta hantering vid incidenter.

2. Inledning

2.1 Bakgrund

Organisationer i offentlig sektor blir alltmer beroende av sina informationssystem. 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*.

2.2. Syfte och revisionsfråga

Granskningen syftar till att besvara följande övergripande revisionsfråga:

Är kommunens organisation och interna kontroll ändamålsenlig och tillräcklig när det gäller IT-säkerhet?

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:

- Finns det en adekvat övergripande styrning av informations- och IT-säkerheten?
- Finns det styrande dokument, såsom policy och riktlinjer för informations- och IT-säkerhet?
- Finns ändamålsenliga rutiner för behörighet och lösenord?
- Upptäcks och hanteras icke önskvärda incidenter både internt och externt på ett ändamålsenligt sätt?
- Hur säkerställs att nya risker och hot identifieras och hanteras?

2.5 Metod och avgränsningar

Granskningen har genomförts genom intervjuer med relevanta roller för granskningen. Vidare har en översiktlig genomgång av riktlinjer och regler kring processen för IT-säkerhet skett. Analys av erhållet material och information från intervjuer har utgjort underlag för en samlad bedömning av den interna kontrollen inom IT-säkerhet kopplat till ovanstående kontrollmål och övergripande revisionsfråga. Analys av information från intervjuer baseras på PwC:s tidigare erfarenhet av granskningar samt god praxis inom området.

Notera att stickprov ej har tagits och att granskningen således är baserad på svaren som gavs under intervjuerna och därmed inte ger några garantier för svarens korrekthet eller fullständighet.

Följande personer har intervjuats i granskningen:

- Christofer Olsson – IT-chef (Töreboda)
- Bengt Sjöberg – Vice ordförande IT-nämnd (Töreboda)
- Per Ahlström – Informationssäkerhetssamordnare och Dataskyddsombud (Gullspång)
- Jonas Bjaaland – Driftkoordinator (Töreboda)

Granskningen har genomförts under september-oktober 2018 av Rolf Svärd (projektledare) och Robin Karlsson, båda från PwC.

Rapporten är faktaavstämd med berörd personal.

3. Resultat av granskningen

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

Iakttagelser

MTG har en gemensam IT-förvaltning med en IT-nämnd som ingår i Töreboda kommuns organisation. Det finns en tydlig rollfördelning och en god samverkan, där IT-nämnden inte är specialister utan förlitar sig på råd från organisationens experter på området. I IT-förvaltningens uppdrag ingår att tillhandahålla drift, support, förvalta system och nätverksmiljö i medlemskommunerna och dess kommunala bolag, samt att arbeta med verksamhetsutveckling. Förutom IT-chefen, som har det samordnande ansvaret för hela IT-förvaltningens verksamhet, finns det en drift- och supportchef. Ansvar för att driva det kommunövergripande informationssäkerhetsarbetet innehas av informationssäkerhetssamordnaren som är organisatoriskt placerad i Gullspång men är en gemensam funktion för MTG. Ansvaret för att upprätthålla informationssäkerheten i verksamheterna följer med det generella verksamhetsansvaret.
Arbetet med den dataskyddsförordningen (GDPR) sköts gemensamt inom MTG, i ett nära samarbete med andra kommuner inom Skaraborg. Dataskyddsombudet innehas i nuläget av samma person som är informationssäkerhetssamordnare.
I dagsläget genomförs det ingen analys av Acceptabel Risknivå som är förankrad med IT-nämnden. På verksamhetsnivå är det respektive verksamhet som fattar beslut om sin risknivå för informationstillgångar
Avseende utbildning har MTG nyligen genomfört e-learnings med samtliga anställda. I nuläget finns inte en långsiktig plan för hur utbildning ska ske avseende informationssäkerhet.
Se avsnitt 3.1. i appendix för mer information om avvikelserna.

Bedömning

Baserat på iakttagelserna är vår bedömning att organisationerna har en delvis adekvat övergripande styrning av informations- och IT-säkerhet. Arbetet leds av Töreboda kommun där IT-förvaltningen är placerad och de har en gemensam informationssäkerhetssamordnare som är placerad i Gullspång. Mot bakgrund av gjorda iakttagelser rekommenderar vi MTG att beakta följande rekommendationer:

PwC rekommenderar MTG att införa en process för att regelbundet analysera, dokumentera och förankra acceptabel risknivå med IT-nämnden. Detta för att ge underlag till IT-nämnden som har till uppgift att säkerställa en hög kvalitet i verksamheten.

PwC rekommenderar MTG att upprätta en utbildningsplan för att säkerställa att alla medarbetare kontinuerligt får utbildning inom informationssäkerhet.

3. Resultat av granskningen

3.2 Finns det styrande dokument, såsom policy och riktlinjer för informations- och IT-säkerhet?

Iakttagelser

MTG har en gemensam *Informationssäkerhetspolicy (reviderad 2017-06-12)* som är antagen av respektive kommun. Respektive nämnd/styrelse i MTG ansvarar för att informationstillgångar inom deras underliggande verksamheter har ett tillräckligt skydd, samt att analysera behovet av och upprättande av regler och rutiner som är nödvändiga för att efterleva informationssäkerhetspolicyn. Kommunchefen ansvarar för att årligen analysera behov av att uppdatera policy.

Kommunerna inom MTG har en *Rutin för informationssäkerhet* (reviderad 2017-12-11) som alla medarbetare ska ta del av och förstå innan åtkomst ges till kommunens nätverk (KIS).

MTG har en gemensam *Metod och mall för informationsklassning* som beskriver klassificering av informationstillgångar. Det finns inte någon kravställning av säkerhetsnivå kopplat till resultatet av klassificeringen. Ur ett användarperspektiv regleras därmed inte hanteringen av informationstillgången. Det saknades även datum för senaste revidering av dokument.

MTG har inte något internt kontrollramverk över IT-kontroller som genomförs inom IT- och informationssäkerhet.

Se område 3.2 i appendix för mer information om avvikelserna.

Bedömning

Vår bedömning är att det finns styrande dokument såsom policy och riktlinjer för informations- och IT-säkerhet på plats som är nödvändiga för att upprätthålla en ändamålsenlig informations- och IT-säkerhet.

Följande rekommendationer lämnas mot bakgrund till iakttagelserna:

PwC rekommenderar MTG att se över befintlig dokumentation där datum för senast revidering saknas. Styrande dokument och riktlinjer för IT- och informationssäkerhet bör granskas regelbundet. Minst en gång per år anser vi att dokumenten behöver revideras för att fortfarande vara aktuella i verksamheten.

PwC rekommenderar MTG att arbeta fram och implementera ett internt kontrollramverk över relevanta kontroller som utförs i organisationerna kopplat till IT.

PwC rekommenderar att MTG utvecklar riktlinjer för kravställning av säkerhetsåtgärder som kopplar till klassificeringen av information. Detta för att medarbetare ska veta hur olika informationsklasser ska skyddas mot obehörig åtkomst.

3. Resultat av granskningen

3.3 Finns ändamålsenliga rutiner för behörighet och lösenord?

Iakttagelser

Beställning av ny, förändrad eller borttag av behörighet görs av respektive chef för användaren. Behörigheter är behovsstyrda vad det gäller användarkonton, administratörsbehörigheter och flertalet av kommunernas applikationer. I nuläget sker detta i form e-post eller pappershantering. Ytterligare digitala alternativ undersöks i nuläget.

Inom MTG har verksamheterna ofta separata system som drivs av verksamheten inom respektive kommun. Behörigheterna för verksamhetssystemen hanteras oftast av verksamhets-administratör för specifikt system på uppdrag av interna chefer. Inom IT-förvaltningen beställs och godkänns behörigheter till drift och infrastruktur av drift- och supportchef.

I nuläget sker ingen kontinuerlig uppföljning av tilldelade behörigheter och att behörigheterna är aktuella och i enlighet med användarens arbetsuppgifter, både för applikationer och infrastruktur. Verksamhetschefer hör ibland av sig till IT-förvaltningen för att kontrollera behörigheter för användare.

Lösenordsparametrarna i Active Directory (AD) är uppsatta utifrån att lösenord är giltiga i 120 dagar samt att lösenord ska vara minst 8 tecken och innehålla minst tre av fyra kategorier av tecken.

Se område 3.3 i appendix för mer information om avvikelserna.

Bedömning

Vår bedömning är att MTG delvis har ändamålsenliga rutiner för behörighet och lösenord. De har en behörighetsstruktur med behovsanpassade roller samt utgår från lösenordsparametrar som är i linje med god praxis.

Samtliga kommuner ställer krav på att nyanställda ska ha läst och förstått rutinen för informationssäkerhet innan de ges åtkomst till kommunens nätverk (KIS).

Utifrån iakttagelserna rekommenderar PwC att MTG minst årligen följer upp användarkonton och behörigheter i applikationer för att säkerställa att endast godkända användare har behörighet, samt att dessa användare har korrekt behörighet i applikationer och för infrastruktur (operativsystem, servrar och databaser), samt att process dokumenteras i styrande dokumentation.

PwC rekommenderar att IT-förvaltningen uppdaterar sin rutin för att hantera upplägg av nya, förändringar av befintliga samt borttag av behörigheter. Rutin bör innefatta hur olika typer av behörigheter hanteras, roller och ansvar, samt hur uppföljning av behörigheter sker. Rutin bör även ha en tydlig koppling till informationssäkerhetspolicyn.

3. Resultat av granskningen

3.4 Upptäcks och hanteras icke önskvärda incidenter både internt och externt på ett ändamålsenligt sätt?

Iakttagelser

MTG har en gemensam *Rutin informationssäkerhet* (se avsnitt 3.2 för ytterligare information), vars målgrupp är samtliga medarbetare. Rutinen innefattar ett avsnitt om betydelsen och tillvägagångssättet för att rapportera incidenter. MTG har även en *Mall för rapportering av informations- säkerhetsincidenter, inklusive personuppgiftsincidenter*. Enligt rutin ska incidenter rapporteras till närmaste chef och ifall incidenter är av IT-relaterad karaktär ska IT-support kontaktas. IT-förvaltningen hanterar incidenter i ärendehanteringssystemet Nilex.

IT-förvaltningen har dokumentation för *Rutin incident* och *Rutin incident akut,* som beskriver hur incidentärendet hanteras från registrering till avslut. Inom IT-förvaltningen har de även uppföljning av IT-relaterade incidenter genom att kvartalsvis gå igenom inträffade incidenter. I dessa forum deltar bland annat IT-chef, Drift- och supportchef och Driftkoordinatorn. Informationssäkerhetssamordnaren involveras i regel inte i arbetet med uppföljning av incidenter, förutom incidenter IT-avdelningen bedömer är allvarliga.

MTG har även utvecklat målgruppsanpassad information gällande informationssäkerhet vars målgrupp är verksamhets- och sektorschefer samt nämnder och styrelser. I dessa dokument beskrivs vilket ansvar rollerna har relaterat till hanteringen av incidenter.

Loggning sker i vissa system i verksamheten och IT-förvaltningen. IT-förvaltningen saknar rutin för att regelbundet granska loggar för trafik som passerar brandväggen.

Se område 3.4 i appendix för mer information om avvikelserna.

Bedömning

Baserat på iakttagelserna är vår bedömning att MTG har en delvis ändamålsenlig process på plats för att upptäcka och hantera incidenter, både inom IT-förvaltningen och verksamheten. Utifrån iakttagelserna rekommenderar PwC följande:

PwC rekommenderar att MTG utreder att övergå till ett enhetligt system för att dokumentera och hantera samtliga inträffade incidenter inom organisationen. I nuläget saknas uppföljning av hur effektivt incidenter hanteras och det sker ingen uppföljning som ger en heltäckande bild av inträffade incidenter. Genom att mäta andelen incidenter som lösts inom en viss tid kan organisationerna följa upp hur arbetet utvecklar sig över tid.

PwC rekommenderar att MTG utreder att inkludera Informationssäkerhetssamordaren i uppföljning av incidenter i större omfattning. Informationssäkerhetssamordnaren har god förståelse för arbetet med informationssäkerhet och kan vara en viktig funktion för att överlappa samarbetet mellan IT, verksamhet och ledning.

PwC rekommenderar IT-förvaltningen att utvärdera behovet av att införa en rutin för och ett system som hjälper till att filtrera loggar för att underlätta granskning av dem. Systemet bör utifrån loggarna indikera vissa förutbestämda mönster som kan tyda på en eventuell attack.

3. Resultat av granskningen

3.5 Hur säkerställs att nya risker och hot identifieras och hanteras?

Iakttagelser

MTG har inte genomfört en övergripande risk- och sårbarhetsanalys för att identifiera väsentliga risker kopplat till IT och informationssäkerhet.

IT-förvaltningen har en påbörjad *Katastrofhanteringsplan* (Disaster Recovery Plan) som innefattar beskrivning för att återställa IT-plattformen och framöver även innefatta beskrivning för att få igång de mest kritiska verksamhetssystemen. Planen innefattar en rutin för att kvartalsvis följa upp och uppdatera planen och uppdaterades senast 2018-01-30. Planen påbörjades på grund av en händelse våren 2016 som framkallade en återstart av IT-plattformen.

Kommunerna har företagsövergripande kontinuitetsplan (BCP) men den saknar en tydlig kravställning till IT. Som nämnts ovan har klassificering av system betydelse även i samband med kontinuitetsplanering, då det är av vikt att veta vilka system som är mest kritiska att få igång först om flera system skulle fallera.

IT-förvaltningen har genomfört riskanalyser för utvalda system och upprättat SLA för kritiska system. IT-förvaltningen har tagit fram en metod för att gå igenom och klassificera system och därigenom identifiera kritiska system. Metoden är inte implementerad. MTG har ingen systemöversikt för att visualisera hela IT-miljön.

Se område 3.5 i appendix för mer information om avvikelserna.

Bedömning

Baserat på iakttagelserna är vår bedömning att MTG delvist arbetar ändamålsenligt med att identifiera och hantera risker och hot, men att MTG kan förbättra processen och möjligheterna för att nya risker och hot identifieras och hanteras på ett mer effektivt sätt.

PwC rekommenderar MTG att kontinuerligt genomföra risk- och sårbarhetsanalys för att identifiera väsentliga risker och hot inom IT.

PwC rekommenderar MTG att färdigställa katastrofhanteringsplanen och säkerställa att uppföljning av plan sker enligt rutin. PwC rekommenderar även att planen kompletteras med roller och ansvar för olika aktiviteter, samt att rutin ses över för uppföljning och uppdatering av dokument. Vi rekommenderar att katastrofhanteringsplanen testas en första gång och därefter årligen genomförs.

PwC rekommenderar MTG att färdigställa och implementera metod för klassificering av system och dokumentera i styrande dokumentation.

PwC rekommenderar IT-förvaltningen att ta fram en systemöversikt för att visualisera hela IT-miljön, innefattande hårdvara, nätverk, mjukvara, beroenden samt övrig relevant information som krävs för att få en god förståelse för befintlig struktur.

.

Datum:

Rolf Svärd
Projektledare

Lars Dahlin
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.
Låg	Syftar på en situation eller arbetssätt som enbart har en begränsad effekt på den interna kontrollen.

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.1	M	PwC noterade att MTG inte har förankrat acceptabel risknivå med IT-nämnden.	Utan en förmedlad acceptabel risknivå från ledningen saknar MTG en nivå och inriktning på risker som ska hanteras respektive kan accepteras i verksamheten.	PwC rekommenderar MTG att införa en process för att kontinuerligt analysera, dokumentera och förankra acceptabel risknivå med IT-nämnden.
3.1	L	Vid vår genomgång noterades att det i nuläget inte finns en långsiktig plan för hur utbildning ska ske avseende informationssäkerhet för medarbetare samt håller sig uppdaterade inom området.	Utvecklingen inom informationssäkerhet går snabbt för att hålla jämna steg med de hot på IT-området som finns mot organisationerna. Om medarbetare inte kontinuerlig utbildas på området så blir deras kunskaper snabbt föråldrade.	PwC rekommenderar MTG att upprätta en utbildningsplan för att säkerställa att alla medarbetare kontinuerligt får utbildning inom informationssäkerhet.
3.2	M	Vi noterade vid vår genomgång att styrande dokument saknade datum för senaste revidering av dokument.	När dokument inte kontinuerligt gås igenom och uppdateras riskerar dem att bli inaktuella, då ökar risken för att de inte är i linje med den IT-/informationssäkerhet som organisationerna behöver.	PwC rekommenderar MTG att se över och vid behov revidera sina befintliga styrande dokument för säkerställa att de fortfarande är aktuella. Vidare rekommenderas att en kontroll införs för att säkerställa att de styrande dokumenten ses över och revideras med viss periodicitet, förslagsvis minst en gång per år.

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.2	M	Det utförs vissa kontroller kopplat till exempelvis behörigheter i verksamhetssystem. Dock saknas övergripande kontrollmatris inom IT för samtliga organisationer.	Vid avsaknad av kontrollmatris ökar risken för att kvalitet, nivå av spårbarhet och utförande av kontroll blir personberoende.	PwC rekommenderar MTG att arbeta fram och implementera en kontrollmatris för relevanta kontroller som utförs i organisationerna kopplat till IT och komplettera med ytterligare kontroller där det är nödvändigt. I kontrollmatrisen bör följande framgå: • På vilket sätt kontrollen skall utföras (kontrollaktivitet och design). • Varför ska kontrollen göras (mål, syfte och vilken risk som hanteras). • Vem som skall utföra kontrollen • Hur ofta skall kontrollen utföras. • Vilken dokumentation skall sparas för att verifiera genomförd kontroll (bevis för spårbarhet). • Vad skall göras om en kontroll uteblir eller är ineffektiv (Åtgärd).

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.2	M	PwC noterade vid granskningen att MTG har en metod för informationsklassning, men saknar riktlinjer för kravställning av säkerhetsåtgärder som kopplar till klassificeringen av information.	Vid avsaknad av klassificering av information riskerar kommunerna att inte veta vilken information som är mest väsentlig och hur denna skall skyddas mot obehörig åtkomst.	PwC rekommenderar MTG att utveckla riktlinjer för kravställning av säkerhetsåtgärder som kopplar till klassificeringen av information. Detta för att medarbetare ska veta hur olika informationstillgångar ska hanteras för att säkerställa krav på tillgänglighet, konfidentialitet och riktighet.
3.3	M	Vi noterade vid vår granskning att det saknas periodvisa genomgångar av behörigheter. PwC har blivit informerade om att det i vissa fall utför informella genomgångar av behörigheter. PwC noterade även att antalet aktiva konton för infrastruktur var fler än antalet anställda på IT-förvaltningen, vilket huvudsakligen berodde på inhyrda konsulter.	Utan en regelbunden granskning av aktuella behörighetsnivåer ökar risken för otillbörlig åtkomst och användning av organisationernas IT-system.	PwC rekommenderar MTG att säkerställa att de årligen genomför en genomgång på sina användare för att säkerställa att endast godkända användare har behörighet, samt att dessa användare har korrekt roll i applikation samt höga/känsliga behörigheter på infrastruktur (operativsystem, servrar och databaser), samt att process dokumenteras i styrande dokumentation.

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.3	M	PwC noterade att det saknas en formell rutin för att hantera upplägg av nya, förändringar av befintliga samt borttag av gamla 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.	PwC rekommenderar att IT-förvaltningen uppdaterar rutin för att hantera upplägg av nya, förändringar av befintliga samt borttag av behörigheter. Rutin bör innefatta hur olika typer av behörigheter hanteras, roller och ansvar, samt hur uppföljning av behörigheter sker. Rutinen bör bygga på att en formell ansökan om behörighet skickas till IT-förvaltningen. Detta bör även gälla vid förändring och borttagande av behörigheter.
3.4	M	PwC noterade vid granskningen att MTG har en fungerande metod för att rapportera informations-säkerhetsincidenter men att de använder en dokumentmall för att rapportera till närmaste chef, och som därefter inte alltid går vidare till IT-förvaltningen eller informationssäkerhets-samordnare.	Om inte alla incidenter registreras på ett enhetligt sätt kan underlag för uppföljning av incidenter bli missvisande. Ökad risk finns för att grundorsaker till en grupp av incidenter inte identifieras och resurser för att lösa återkommande incidenter felprioriteras, vilket även kan leda till omotiverade kostnader.	PwC rekommenderar att MTG utreder att införskaffa ett system för att dokumentera och underlätta hantering av inträffade incidenter. I nuläget saknas uppföljning av hur effektivt olika typer av incidenter hanteras och det sker ingen uppföljning som ger en heltäckande bild av inträffade incidenter. Genom att mäta andelen incidenter som lösts inom en viss tid kan organisationerna följa upp hur arbetet utvecklar sig över tid.

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.4	L	PwC noterade att informations-säkerhetssamordnaren, baserat på styrande dokumentation, inte har en tydlig roll i hantering och uppföljning av incidenter.	Informationssäkerhetssamordnaren har god förståelse för arbetet med informationssäkerhet och kan vara en viktig funktion för att överlappa samarbetet mellan IT och verksamhet. Relevant kompetens riskeras att inte nyttjas.	PwC rekommenderar att MTG utreder informationssäkerhetssamordarens roll i hantering och uppföljning av incidenter.
3.4	M	MTG saknar rutin för att regelbundet eller systemmässigt granska trafik som passerar brandväggen.	Utan en rutin eller ett systemstöd för att kontinuerligt granska loggar finns en risk att man inte upptäcker eventuella intrångsförsök mot verksamheten. Detta medför att en eventuell angripare kan genomföra attacker utan risk för upptäckt.	PwC rekommenderar IT-förvaltningen att utvärdera behovet av att införa en rutin för och ett system som hjälper till att filtrera loggar för att underlätta granskning av dem. Systemet bör utifrån loggarna indikera vissa förutbestämda mönster som kan tyda på en eventuell attack.
3.5	H	PwC noterade vid genomgången att organisationerna ej har genomfört övergripande risk- och sårbarhetsanalys övergripande för IT.	Om organisationerna ej kontinuerligt genomför risk- och sårbarhetsanalyser riskerar dem att missa nyuppkomna hot eller interna sårbarheter mot IT-säkerheten.	PwC rekommenderar MTG att genomföra en risk- och sårbarhetsanalys kopplad till IT-säkerhet. Samt att säkerställa att analysen kontinuerligt följs upp och hålls uppdaterad.

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.5	M	PwC noterade att IT-förvaltningen har en påbörjad Katastrofhanteringsplan som innefattar beskrivning för att återställa IT-plattform och återstarta de mest kritiska verksamhetssystemen. Vidare noterades att vissa kommuner har kontinuitetsplan (Business Continuity Plan) för sin verksamhet men att kravställning mot IT är otydlig.	Om det ej finns katastrof- eller kontinuitetsplan implementerade riskerar organisationerna att vara oförberedda samt att förlora dyrbar tid i händelse av katastrof.	PwC rekommenderar IT-förvaltningen att färdigställa Katastrofhanteringsplanen och säkerställa att uppföljning av plan sker enligt rutin. PwC rekommenderar även att planen kompletteras med roller och ansvar för olika aktiviteter, samt att rutin ses över för uppföljning och uppdatering av dokument, samt hur ofta planen ska testas.
3.5	M	PwC noterade vid genomgången att organisationen har tagit fram en metod för klassificering av system men att denna ännu inte implementerats.	En svagt dokumenterad IT-miljö innebär ökade risker vid personalomsättning samt onödiga extrakostnader vid inköp av nya system och applikationer.	PwC rekommenderar MTG att fortsätta arbetet med att implementera metod för klassificering av system och dokumenteras i styrande dokumentation. Systemdokumentationen bör beskriva nätverk, hårdvara, mjukvara, beroenden samt övrig relevant information som krävs för att få en god förståelse för befintlig struktur.

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.5	M	PwC noterade vid genomgången en avsaknad av fullständig systemöversikt, dvs vilka applikationer, system och nätverkskomponenter som finns inom MTG samt hur dessa kommunicerar.	En svagt dokumenterad IT-miljö innebär ökade risker vid personalomsättning samt kan innebära onödiga kostnader vid inköp av nya system och applikationer. Vidare kan en bristfällig förståelse för IT-miljön öka risken för störningar i IT-system då uppgraderingar ska genomföras.	PwC rekommenderar IT-förvaltningen att ta fram en systemöversikt för att visualisera hela IT-miljön, innefattande hårdvara, nätverk, mjukvara, beroenden samt övrig relevant information som krävs för att få en god förståelse för befintlig struktur.