Intern kontroll av IT-miljön på Trollhättans Stad

Iakttagelser ifrån IT Revision – del av löpande granskning 2019

December 16, 2019

Building a better working world

Innehåll

Introduktion

Bakgrund

Att förstå Trollhättans stads användande av IT, samt rollen IT spelar för stadens processer och verksamhet, är ett viktigt steg för att bestämma den översiktliga revisionsstrategin samt att utföra en effektiv revision av hög kvalitet. IT utgör grunden för driften av finansiella och kommersiella processer i flera avseenden, från enkla beräkningsverktyg såsom Microsoft Excel, till användandet av komplexa förprogrammerade finanslösningar såsom Unit4 Business World(härefter benämnt UBW).

Som en del av den finansiella revisionen av Trollhättans stad för revisionsåret som slutar 2019-12-31 har en genomgång genomförts av relevanta processer (såsom behörighetstilldelning, ändringshantering och drift) i följande IT-applikationer:

- UBW, dvs. Unit4 Business World

Denna genomgång har genomförts genom att en generell förståelse för relevanta IT-processer har etablerats och tillhörande riskexponering har utvärderats.

Innehåll

Denna rapport beskriver våra iakttagelser kring förbättringsområden inom Trollhättan Stads IT-processer, d.v.s. tillfällen där IT-processer har saknat adekvat kontrollaktivitet för att adressera den identifierade risken. Detta betyder att det finns en realistisk risk att materiella fel skulle kunna uppstå i IT-miljön som inte hade kunnat förebyggas eller förutsägas inom rimlig tid för det dagliga arbetet i Trollhättans stads verksamhet. Syftet med våra iakttagelser, riskbeskrivningar och rekommendationer i detta pm är att uppmuntra och stödja förbättring för internkontroll i Trollhättans stads IT-miljö.

Begränsat användande

Detta pm utgör inte en formell åsikt om Trollhättans interna kontroll eller finansiella rapporteringsstruktur och kan därmed inte användas som intyg för effekten och kvalitén på Trollhättans stads kontrollmiljö.

Iakttagelser 2019

1. Tilldelning samt ändring av applikationsbehörighet är inte formaliserad

Observation	Det har identifierats att processen för tilldelning och förändring av behörigheter inte är formaliserad. Informella processer existerar och är i viss mån kommunicerade inom organisationen. I dagsläget inkommer en förfrågan via mail ifrån organisationen till systemadministratör, med behörighet att tilldela roller och atttestbehörighet. Systemadministratör har kommunicerat till organisationen att endast ekonomiansvariga har rätt att efterfråga behörighet till en användare. Denna process är emellertid inte dokumenterad som arbetssätt och det saknas även spårbarhet, speciellt kopplat till rutiner för att upprätthålla segregation av roller och/eller attestbehörigheter. I dagsläget ligger det på systemadministratör att avgöra huruvida en segregationskonflikt skulle kunna uppstå vid tilldelning.
Risk	Utan en formaliserad process finns det en risk att användare får möjlighet att obehörigt se och ändra kritisk information som en följd av bristande kontroll av behörighetstilldelning.
Rekommendation	Det rekommenderas att Trollhättans stad implementerar en process supporterad med dokumentation som beskriver processens olika steg för tilldelning och ändring av behörigheter och attesträtter. Till processen behövs även en dokumenterad matris som beskriver otillåtna kombinationer av attesträtter och behörigheter som kan ligga till stöd för systemadministratörens analys av segregationskonflikt vid tilldelning.
Kommentar ifrån Trollhättans stad	Arbetet med att formalisera rutiner för att minimera risker kommer påbörjas under 2020. En möjlig lösning skulle vara att sätta upp en rutin i systemet Flexite(ett system som administreras av IT-avdelningen) för att säkerställa att behörig person utser attestanter som sedan lämnas till systemansvarig för upplägg. I ett sådant fall skulle detta även samtidigt dokumenteras. Matris för segregationskonflikter kan ses över i detta arbetet.

2. Periodisk genomgång av användare är inte genomförd eller formaliserad

Observation	Det har identifierats att det saknas en formell process för att periodiskt gå igenom användares behörigheter och attesträtter för att säkerställa att dessa är riktiga och kompletta. I dagsläget finns det ingen formaliserad process och det utförs heller ingen periodisk genomgång av behörigheter och attesträtter. Detta är speciellt problematiskt med tanke på att UBW har 800–900 användare med viss attesträtt och att ändringar/tillägg sker flera gånger dagligen.
Risk	Utan en formaliserad process finns det en risk att användare får möjlighet att obehörigt se och ändra kritisk information som en följd av bristande kontroll av behörighets- och attest tilldelning.

Rekommendation	Det rekommenderas att Trollhättans stad implementerar en formaliserad process för periodisk genomgång. Processen bör genomgå behörighet och attesträtt på rollnivå, dvs. inte endast verifiera om personer fortfarande arbetar kvar och bör vara användare. Periodisk genomgång av alla användarbehörigheter och attesträtt bör genomföras årligen. Användarbehörighet och attesträtt, som är identifierade som kritiska, bör göras minst två gånger per år. Genomgången bör utgå ifrån en systemgenererad lista av användare. Listan bör genomgås av relevanta chefer eller ansvariga inom organisationen. Genomgången bör dokumenteras, godkännas av utförarna och lagras för att säkerställa spårbarhet.
Kommentar ifrån Trollhättans stad	Arbetet med att formalisera processen kommer att påbörjas under 2020. Ekonomisystemet har stöd för att göra sådana kontroller.

3. Processen för hantering av ändringar i UBW är inte formaliserad

Observation	Det har identifierats att processen för ändringshantering inte är formaliserad för IT-systemet UBW. Detta inkluderar både systemändringar och direkta ändringar i databaser. Det saknas till exempel en dokumenterad rutin för initiering, testning, godkännande och implementation av ändringar. I dagsläget har endast mindre ändringar skett i UBW eftersom det implementerades först 2018. Det har också skett en större systemuppdatering ifrån version Spring 2016.3 till Spring 2016.4 (en uppgradering av systemet som innefattar mindre ändringar och buggfixar, men även större ändringar såsom utvecklad eller adderad funktionalitet), men fler och större ändringar väntas ske under det kommande året. Det har även identifierats att systemleverantören tillåts genomföra direkta ändringar i databasen för UBW, som inte hanteras och dokumenteras på något strukturerat vis.
Risk	Avsaknaden av en tydlig ändringsprocess utan möjlighet att se spårbarhet i utvecklingsaktiviteter ökar risken för att obehöriga ändringar implementeras.
Rekommendation	Det rekommenderas att Trollhättans stad implementerar en rutin för ändringshantering där alla ändringar ska initieras genom ett formellt ändringsförslag i ett ärendehanteringssystem. Testning ska sedan genomföras och dokumenteras. Varje ändringsförslag ska få ett formellt godkännande och dokumenteras innan ändringen implementeras. Om processen skiljer sig för olika typer av ändringar så bör det framgå i rutinen. Vidare bör inte gruppkonton med behörighet till produktionsmiljön tillåtas.
Kommentar ifrån Trollhättans stad	Under hösten påbörjades ett arbete tillsammans med IT-avdelningen för att strukturera ansvarsfördelning för förändringar i systemet och då startades ett rum i sharepoint för att kunna påbörja arbetet med formerna för framtida förändringar.

4. Processen för återläsningstester av säkerhetskopieringar genomförs inte som planerat

Observation	Det har identifierats att den formaliserade processen för återläsningstester av säkerhetskopieringar har en upplevt stora förseningar under året. Det är i dagsläget inte fastställt om detta är en följd av en ineffektiv process eller felaktigt prioriterat. Säkerhetskopieringar sker i utställd takt.

Risk	Avsaknaden av en fungerande process för återläsning av säkerhetskopieringar ökar risken att, för verksamheten kritisk information, går förlorad.
Rekommendation	Det rekommenderas att Trollhättans stad ser över processen för återläsningstester och utarbetar en handlingsplan för att komma till rätta med förseningarna som den nuvarande processen upplever.
Kommentar ifrån Trollhättans stad	Kommer att läggas in i förvaltningsplan för att ske årligen.

5. Processen för övervakning av schemalagda jobb är inte formaliserad på systemnivå[1]

Observation	Det har identifierats att det inte finns någon process för övervakning av schemalagda jobb i UBW. Det finns andra initiativ som övervakar server- och nätnivån av IT-miljön men dessa initiativ täcker inte systemnivån.
Risk	Avsaknaden av en formaliserad process för övervakning av schemalagda jobb ökar risken för att allvarliga systemfel inte upptäcks i tid och/eller kan förebyggas.
Rekommendation	Det rekommenderas att implementera en formaliserad process för övervakning av schemalagda jobb. Denna process bör inkludera en mappning av kritiska schemalagda jobb och en dokumentation av händelser, uppföljning och lösning.
Kommentar ifrån Trollhättans stad	OP5, ett system som IT har tillgång till, kan övervaka schemalagda jobb, har inte implementerats ännu.

6. Processen för incidenthantering är inte formaliserad på systemnivå

Observation	Det har identifierats att det inte finns någon formaliserad process för att hantera incidenter i UBW. Incidenter hanteras *ad hoc* och på reaktiv basis i dagsläget. Process för att förebygga incidenter saknas.
Risk	Avsaknaden av en formaliserad process för incidenthantering ökar risken för allvarliga systemfel inträffar som kan orsaka långa avbrott för system som är kritiska för verksamheten.
Rekommendation	Det rekommenderas att Trollhättans stad implementerar en incidenthanteringsprocess för UBW. Denna process bör vara i linje med den översiktliga incidenthanteringsprocess som är implementerad på server- och nätverksnivå.
Kommentar ifrån Trollhättans stad	Vi får påbörja arbetet med att bättre dokumentera åtgärder vid eventuella incidenter för att bättre kunna förbeygga att de återupprepas.

7. Bristande process för verifiering och accesshantering av konsulter

Risker har identifierats inom detta område. Rekommendationer har lämnats till berörd verksamhet.

[1] Schemalagda jobb är aktiviter som genomförs av ett system vid en schemalagd tidpunkt för att jämna ut systemanvädningen och på så vis minska risken för överbelastning. Exempel på schemalagda jobb i ett finansiellt system såsom UBW är utbetalning av löner, uppdatering av användarlistor, bokföring av försäljningsordrar etc.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

ey.com