Deloitte.

Granskning av IT Säkerhetsarbete

Härnösands kommun

Socialnämnden, Arbetslivsnämnden, Samhällsnämnden

Innehåll

Sammanfattning

Uppdrag och bakgrund
En granskning på kommunövergripande nivån i november 2017 visade ett pågående utvecklingsarbete avseende IT säkerhetsarbetet. Inaktuella riktlinjer och avsaknad av övergripande kontrollfunktion, med uppmärksammade risker som följd, har lett till att granskningen utvidgats till att omfatta nämndnivån. En god intern kontroll är viktig för att kunna uppnå och upprätthålla en hög IT-säkerhetsnivå och minimera riskerna för att verksamheten ska drabbas av allvarliga störningar.

Syfte
Syftet med granskningen har varit att se hur nämnder/ förvaltningar arbetar med det systematiska IT-säkerhetsarbetet. Ett antal kontrollfrågor har ställts med uppföljande kontakter kring svaren.

Revisionskriterier
Grund för bedömningar utgörs främst av relevant lagstiftning samt interna styrdokument.

Svar på syfte och revisionsfrågor
De risker som uppmärksammats i tidigare granskning har stärkts genom konstaterade brister inom IT-säkerhetsarbetet på nämnd/förvaltningsnivån.

Rekommendationer
Efter genomförd granskning rekommenderar vi att:

- Förteckningar av systemägare, systemförvaltare uppdateras och ajourhålls.
- IT-säkerhetsinstruktioner samt IT-säkerhetspolicy uppdateras och ajourhålls.
- Behovet av fora för hantering av olika systemfrågor och erfarenhetsutbyte mellan systemförvaltare/systemägare lyfts.
- Erforderlig dokumentation gällande behörighets-administration upprättas (av särskild vikt där arbetet utförs av enskilda individer och är av manuell karaktär).
- Backuper som återlästs och testats enligt rutinen genomlyses och dokumenteras.
- Kontrollåtgärder av ”IT säkerhetsinstruktion användare” genomförs på individnivån. Utred om en standardiserad process för arbetet behövs.
- Analyser av säkerhetslogg vid samhälls- och arbetslivs-förvaltningen dokumenteras.
- Ansvar och roller ses över och förtydligas.
- Beslut om årliga mål tas i enlighet med policyn.

DELOITTE AB

Härnösand	2018-03-14
Mathias Gordonsson	Marianne Harr
granskningsledare	projektledare

1. Inledning

1.1. Uppdrag och bakgrund

En god intern kontroll är viktig för att kunna uppnå och upprätthålla en hög IT-säkerhetsnivå och minimera riskerna för att verksamheten ska drabbas av allvarliga störningar.

På uppdrag av de förtroendevalda revisorerna har Deloittte granskat den interna kontrollen avseende IT-säkerhets-arbetet på nämnd/förvaltningsnivå.

1.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om den interna kontrollen avseende IT-säkerhetsarbetet är tillräckligt.

Inom ramen för granskningens övergripande syfte ska granskningen besvara kontrollmål enligt bilaga till rapporten (IT säk HK).

1.3. Revisionskriterier

Revisionskriterierna är de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

I denna granskning har revisionskriterierna huvudsakligen utgjorts av:

- IT-säkerhetspolicy – 120827
- IT-säkerhetsinstruktion Förvaltning
- IT-säkerhetsinstruktion Drift
- IT-säkerhetsinstruktion Användare
- Erhållna svar IT säk HK

1.4. Metod

Granskningen har genomförts genom att skriftliga frågor sänts till respektive förvaltningschef enligt underlag IT säk HK. Svar har kommit via IT utvecklare/förvaltningschef från social-, arbetslivs- och samhällsförvaltningen. Uppföljande kontakter kring förtydliganden har tagits.

Skolförvaltningen har efter påminnelser inte lämnat svar varför skolnämnden inte omfattas av granskningen.

Hänsyn har tagits till granskningsresultat i nyligen genomförd granskning (november 2017) avseende kommunövergripande nivån.

2. Granskningsresultat

2.1. Iakttagelser

Nedan redovisas iakttagelser för respektive nämnd/förvaltning utifrån granskningens kontrollmål i bilaga.

Socialförvaltningen

System, Behörigheter
Vi har noterat att behörighetsadministration inte genomförs på ett likvärdigt sätt för alla system som förvaltningen använder exempelvis kvalitets- och ledningssystemet Stratsys, 2c8, Journal Digital, Alk-T. För förvaltningens större verksamhetssystem som Procapita, Treserva, Prator går beställningar via Nilex. I det senare fallet har ett systematiskt arbetssätt kopplat till behörigheter införts.

Kontroller kopplat till behörigheter och användare genomförs, dock inte efter någon fastställd rutin eller intervall. Systemförvaltare registervårdar efter information om anställningens förändring eller vid uppenbara inaktuella uppgifter. Information om användare och behörigheter finns i respektive system och det krävs systemförvaltarbehörighet för att kunna se uppgifterna.

Någon dokumentation kopplat till de specifika behörigheter en användare har finns inte i dagsläget. Detta är en brist som förvaltningen är medveten om. Ansvaret för kontrollprocessen är inte tydlig enligt uppgifter.

En systematisk logguppföljningsrutin har införts från och med 2018 som inte funnits tidigare med undantag för vissa verksamheter och system. Logguppföljningarna kommer att ske tertialvis och följas upp som en egenkontroll i kvalitets- och ledningssystemet Stratsys.

Vi har noterat att det saknas systembeskrivningar på förvaltningsnivå utöver den övergripande förvaltningskatalog som centrala IT tillhandahåller.

Kontrollrutiner
Av IT säkerhetsinstruktion för förvaltning framgår att ”systemägaren ansvarar för att återläsningskontroll utförs regelbundet”.

Utan dokumentation av tester från utförda backuper av en applikation finns det inga spår som kan verifiera att backupen verkligen fungerar som det är tänkt. Vid otillräcklig testning kan oplanerade fel uppstå och funktionaliteten kanske inte möter användarnas behov eller att felet tar längre tid att åtgärda än vad verksamheten förväntat sig.

I tidigare granskning erhölls informationer om att riktlinjer finns men att efterlevnaden varierar beroende på system. I förvaltningens svar hänvisas till att hanteringen underhålls och utförs av centrala IT. Av riktlinjerna framgår att centrala IT enbart svarar för utföra säkerhetskopiering utifrån det intervall som systemägaren bestämt och har därmed inte ansvar för återläsningstest.

Förhållningssätt
Förvaltningen har inga egna mål gällande IT säkerhets-arbetet och känner inte till om det finns några centralt i kommunen.

När det gäller roller och ansvar för systemägare görs hänvisning till ”IT-säkerhetsinstruktion för Förvaltning” som anses vara styrande. Vi kan av ovan lämnade beskrivning kring återläsningskontroll konstatera att ansvarsfördelningen uppfattas otydlig. Övergripande fora för erfarenhetsutbyten saknas i dagsläget enligt uppgifter.

En webbaserad introduktionsutbildning håller på att färdigställas som innefattar IT säkerhet och vad som gäller för de som arbetar i verksamhetssystem. Utbildningen kommer att innehålla ett kunskapstest för att verifiera deltagandet och förståelsen.

Utvecklingsarbeten
Förvaltningen kommer under våren 2018 att påbörja ett arbete med översyn av behörigheterna. Genom att definiera och dokumentera behörigheter önskar verksamheten att renodla samt tydliggöra de systembehörigheter som används. Målbilden är att beställande chef ska känna till och aktivt välja vilken behörighet den anställde ska ha. Idag består beställningen endast av information om vilket system användaren ska ha åtkomst till. Systemförvaltaren tilldelar behörighet utifrån vilken funktion och enhet användaren tillhör.

Förvaltningen har under längre tid lyft frågan till centrala IT om behovet av behörighetshanteringssystem. Förslag på programstöd finns och kallas för IAM, Identity Access Management. Systemet medger valbarhet för olika behörigheter och möjligheter till loggning av beställningar, förändringar och avslut. Närmaste chef ges översikt och kontrollmöjligheter som inte erhålls i dagsläget. Via IAM ges möjligheter att automatisera användargenomgångar med givna intervall där chefen enkelt kan se vilken behörighet dess personal har och begära förändringar eller avslut.

Arbetslivsförvaltningen

System, Behörigheter
Vi har noterat att behörigheter hanteras centralt på alla system förutom till lärplattformen Itslearning och Dexter där behörigheter hanteras av systemadministratörer inom förvaltningen.

Enligt förvaltningen hanteras behörigheter på ett standardiserat sätt. Vid förvaltningen kan man i alla system se vilken behörighet som delgivits varje unik användare. Vi har noterat att det inte finns någon dokumentation kopplat till vilka specifika behörigheter en användare har utöver att utföra enskilda kontroller i respektive system.

Kontroller av behörigheter och användargenomgångar sker dels per automatik baserat på tillhörighet för anställningen och dels görs kontroller av användare av systemadministra-törer. Dokumentation kring ovan redovisade process saknas.

Kontrollrutiner
Se motsvarande avsnitt under socialförvaltningen.

Förhållningssätt
Vi har noterat att kontroller gällande efterlevnad av IT säkerhetsregler inte utförs vid förvaltningen. Reglerna ingår som en del i introduktionsutbildningen enligt uppgifter. Någon form av dokumentation som styrker att användarna tagit del av reglerna har inte förevisats.

Övergripande fora för system och erfarenhetsutbyte kopplat till kommunens IT säkerhetsarbete hanteras av centrala IT tillsammans med IT-samordnare. Någon återföring i form av

dokumentation/kommunikation i förvaltningen har inte förevisats. Förvaltningsspecifik dokumentation kring ansvar och roller för systemägare saknas.

Mål som rör IT säkerhet finns i förvaltningens IT plan och följs upp i boksluten. Det är inte klarlagt om man känner till på det sätt målen är kopplade till långsiktiga mål i IT säkerhetspolicyn.

Regler rörande IT säkerhet utgör en del av introduktions-utbildningen inom förvaltningen. Det sker inga kontroller av att anställda känner till eller har tagit del av reglerna.

Samhällsförvaltningen

System, Behörigheter
Vi har frågat efter förvaltningens arbeten med kontroll av behörigheter och användargenomgångar. Användare och deras behörigheter hanteras i verksamhetssystem. Enligt förvaltningen utförs manuella kontroller i systemen. Någon dokumentation kring ovan redovisade process har inte förevisats. Informationer har lämnats om att det saknas systemstöd för att säkerställa likvärdighet i dagsläget.

Kontrollrutiner
Se motsvarande avsnitt under socialförvaltningen.

Förhållningssätt
Några kontroller gentemot regler för IT säkerhet görs inte. Rutiner för att säkerställa att användare tagit del av och förstått reglerna finns inte. Dokumentation i form av förteckningar kring roller och ansvar saknas. Lista avseende systemägare för användare finns men är bristfällig enligt uppgifter.

Förvaltningen har inte tagit fram några mål kopplade till långsiktiga mål i IT säkerhetspolicyn. Förvaltningen önskar samordning och gemensamma grepp på kommun-övergripande nivån avseende IT säkerhetsarbetet.

Skolförvaltningen

Skolförvaltningen har efter flera påminnelser inte lämnat svar vid rapporttillfället och omfattas inte av rapporten.

3. Bedömning och rekommendationer

3.1. Bedömningar

Vi bedömer att interna kontrollen avseende IT-säkerhetsarbetet erfordrar förbättringar.

Granskningen visar att ansvarsfördelningen för kommunens IT-system finns dokumenterad (förvaltningskatalog med system, systemägare samt systemförvaltare). För varje system utses en systemägare enligt ”IT-säkerhetsinstruktion för förvaltning”. Förteckningar över vilka personer/ funktioner som är systemägare för olika system finns men är inaktuella enligt uppgifter. Rutin för att uppdatera och ajourhålla förteckningar behövs. I erhållet underlag saknas systemägare för skolförvaltningens system.

Samtllga styrdokument, som varit underlag i granskningen, är inaktuella då giltighetstiden passerat (IT säkerhets-instruktioner samt IT säkerhetspolicy). Dokumenten håller på att revideras enligt IT-chefen.

Av ”IT-säkerhetsinstruktion för förvaltning” framgår att systemägaren ansvarar för att återläsningskontroll utförs regelbundet. Granskningen har ej kunnat styrka någon regelbunden hantering eller att återläsningskontroller görs. Indikationer lämnas kring en osäkerhet på det sätt arbetet utförs.

Den interna kontrollen bör kunna stärkas via genomlysning kring de systembackuper som återläses och med vilken regularitet samt att processen dokumenteras.

Socialförvaltningens införande av en systematisk logguppföljningsrutin från och med 2018 stärker kontrollen. Logguppföljningarna sker tertialvis och följs upp som en egenkontroll i kvalitets- och ledningssystemet Stratsys.

Dokumenterade rutiner och mallar för hantering av behörigheter till kommunens samtliga IT-system saknas. Socialförvaltningen har fört fram önskemål om kontrollåtgärder för att underlätta tillämpningen av behörighetsadministration till centrala IT. Förslag på införande av programstöd, IAM system (Identity Access Management), har lämnats.

Utifrån att samtliga förvaltningar utför manuella behörig-hetskontroller i flertal använda system bör rutiner för att stärka internkontrollen övervägas (med programstöd eller på annat sätt). Underliggande dokumentation som styrker innehåll och genomförande av manuella kontroller har inte förevisats.

IT-säkerhetsutbildning för kommunens anställda är ett särskilt viktigt område enligt IT säkerhetspolicyn. Alla användare skall ges kunskap om gällande dokument ”IT säkerhetsinstruktion för användare”. Rutiner för att förmedla innehållet ser olika ut i granskade förvaltningar. Några underlag som styrker att de anställda har tagit del av informationen har inte lagts fram. Internkontrollen bör kunna stärkas för att leva upp till policyns intentioner.

3.2. Rekommendationer

Efter genomförd granskning rekommenderar vi att:

- förteckningar och systemägare, systemförvaltare uppdateras och ajourhålls
- IT-säkerhetsinstruktioner samt IT-säkerhetspolicy uppdateras och ajourhålls enligt fastställda rutiner.
- behovet av fora för hantering av olika systemfrågor och erfarenhetsutbyte mellan systemförvaltare/ systemägare lyfts.
- erforderlig dokumentation gällande behörighets-administration upprättas (av särskild vikt där arbetet utförs av enskilda individer och är av manuell karaktär).
- backuper som återläst och testats enligt rutinen genomlyses och dokumenteras.
- kontrollåtgärder gällande uppföljning av ”IT-säkerhetsinstruktion användare” genomförs på individnivå samt utreda om en standardiserad process för detta arbete är möjligt eller önskvärt.
- analys av säkerhetslogg dokumenteras. Pågående arbete vid socialförvaltningen med automatisk logguppföljning förbättrar egenkontrollen. Arbetet kan med fördel anpassas till övriga förvaltningar som har liknande behov. Frågan kring dokumenterad analys av säkerhetlogg har inte besvarats av arbetslivs- och samhällsförvaltningen vid rapporttillfället.
- fastställa årliga mål i enlighet med policyn. Mål finns uttryckta i arbetslivsförvaltningens IT-Plan, dock inte i verksamhetsplan. Social- och samhällsförvaltningen har inte gett uttryck för mål kopplat till IT säkerhets-arbetet i den årliga verksamhetsplanen.