Deloitte.

Granskning av IT säkerhet 2017

Kommunstyrelsen

Revisionsrapport 2017-11-08

Sammanfattning

I denna rapport sammanfattas resultatet av granskning av IT säkerhet. Granskningen har avgränsats till kommunstyrelsen och kommunövergripande nivån. Granskningens syfte är att undersöka och bedöma internkontrollen genom det systematiska IT säkerhetsarbetet.

Riktlinjer i IT säkerhetspolicyn är inaktuella och håller på att revideras. Arbeten med införandet av ledningssystem för informationssäkerhet (LIS) pågår. Riktlinjer, förhållningssätt och dokumentationsstandarder kring säkerhetsarbetet kommer att kunna hanteras inom pågående arbeten.

I granskningen har risker kring att riktlinjer inte hålls aktuella eller följs upp uppmärksammats. Det gäller också risker vid avsaknad av en övergripande kontrollfunktion. Det är nödvändigt att ansvariga på respektive nivå är informerade om rutiner och de kontroller som faktiskt utförs i ett fungerande säkerhetsarbete. Brister i rutiner och dokumentation från utförda kontroller har framkommit. Bristande rutiner och kontroller kan leda till att avsikter och mål med säkerhetsarbetet inte uppnås.

Bedömning

Vi har bedömt att internkontrollen för det systematiska IT säkerhetsarbetet erfordrar väsentliga förbättringar.

Intern kontroll

Bedömningen grundas enligt följande

- Erfordrar väsentliga förbättringar
- Erfordrar förbättringar
- Tillfredsställande mindre iakttagelser
- Tillfredsställande

IT Säkerhet

Granskning	Resultat
IT säkerhetspolicy	Riktlinjer för säkerhetsarbetet finns i IT-säkerhetspolicyn (2012). Befintliga underlag i IT säkerhetspolicy med tillhörande IT säkerhetsinstruktioner saknar aktualitet (giltiga t o m 2016-12-31) och håller på att ses över enligt uppgifter. Granskningen har omfattat frågor inom nedan områden: • Riktlinjer, rutiner, anvisningar • Ansvarsfördelningen • Uppföljning • Rapportering Säkerhetsinstruktioner finns framtagna för förvaltning, kontinuitet och drift och användare. I dagsläget utförs inte någon uppföljning gällande efterlevnad av riktlinjerna enligt uppgifter. Anvisningar/instruktion kring standardiserade tester (backup/restore) finns och efterlevnaden sägs variera beroende på system.
Risk Ansvarsfördelning	*Vid avsaknad av uppföljning av efterlevnad i riktlinjer ökar risker för att kraven inte upprätthålls och efterlevs.* Ansvarsfördelningen är klarlagd och dokumenterad i policyn. IT chef är systemägare för det interna IT nätverket. IT tekniker vid IT enheten svarar tillsammans med systemägare och systemförvaltare för att den dagliga driften upprätthålls. Det övergripande ansvaret för IT-systemen vilar på respektive förvaltningschef som också utser systemägare för organisationens IT-system. Systemägaren ansvarar för att systemsäkerhetsanalyser för de egna informationssystemen genomförs.

IT säkerhet

Granskning	Resultat
	Något övergripande fora för system och erfarenhetsutbyte kopplat till kommunens IT-säkerhetsarbete finns inte. Någon ansvarig person vid IT enheten för övergripande kontroller avseende IT säkerhetsarbetet har inte utsetts.
Uppföljning av mål	Mål i policyn ska följas upp av respektive förvaltning. Det är idag inte klarlagt vilka årliga mål i policyn som fått genomslag i förvaltningarnas verksamhetsplanering kopplat till IT-säkerhetsarbetet.
Risk	*Vid avsaknad av övergripande kontrollfunktion ökar risker att fastställda mål och krav inte följs/upprätthålls och efterlevs på avsett sätt.*
Informations-klassning	Informationsklassning är en metod som hjälper verksamheten att välja rätt skyddsåtgärder för sin information, exempelvis personuppgifter. Ett arbete kopplat till införande av ledningssystem för informationssäkerhet (LIS) pågår. Ett antal frågor kopplat till området har ställts. IT-chef har informerat om att samtliga frågor kommer hanteras inom ramen för detta arbete. Nedan redovisas frågor som kommer hanteras inom pågående arbete (LIS) • Informationsklassning, finns fastställd standard/dokumentation/riktlinjer för hur detta arbete genomförs? • Finns någon standardiserad dokumentation/förhållningssätt som säkerställer att upprätthåller önskad säkerhet? • Finns ett standardiserat förhållningssätt kopplat till driftgodkännande av systemägaren? • Finns dokumentation kring när ett system validerats/godkänts för skarp drift?

IT säkerhet

Granskning	Resultat
Incident/ Behörighet	Incidenter ska rapporteras till IT enhet eller närmaste chef. Systemägaren har att följa konsekvenserna av den och verka för att det inte uppkommer igen. Systemägaren beslutar även om vem som ska få tillträde och med vilken behörighetsnivå till IT-systemen. Rutin för eskalering/incidenthantering finns och är bristfälligt beskriven enligt uppgifter. Utan tydliga eskaleringsvägar ökar risker för att olika incidenter inte rapporteras. Vi har noterat att det utförs sporadiska användargenomgångar på systemnivå.
Risk	*Brister i eskaleringsrutin kan medföra att eventuell rapportering inte genomförs inom en för verksamheten acceptabel tidsram.* *Ej konsistent användaradministration kan leda till att användare får felaktiga behörigheter eller har access till icke önskvärd systemfunktionalitet.*
Utbildning	Av policyn följer att IT-säkerhetsutbildning för kommunens anställda är ett särskilt viktigt område. Alla användare skall ges kunskap om gällande dokument ”IT säkerhetsinstruktion för användare”. Vi har i vår granskning noterat att ingen dokumentation finns om kommunens anställda tagit del av någon av dessa områden.
Risk	*Vid avsaknad av utbildning ökar risker för att fastställda krav inte upprätthålls och efterlevs på ett för verksamheten ändamålsenligt sätt.*