§ 110 Dnr KS 2022/00929-1.6.1

Beslut - Revisionsrapport 2022:5, Granskning av IT- och informationssäkerhet

Beslut

Förslag till kommunfullmäktige:

1. Stadsledningskontorets förslag till yttrande daterat 2024-02-28 antas och lämnas över till Västerås stads revisorer.

2. Revisionsrapporten läggs till handlingarna

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation.

Rapporten lämnades till kommunstyrelsen den 9 mars 2023 och har remitterats till samtliga nämnder i staden, vilka sedan inkommit med yttranden.

I granskningen har förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen följande:

• En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

• En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

• En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Västerås stad bedömdes ha en genomsnittlig mognadsgrad på 2,50, vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52.

De remitterade nämnderna och stadsledningskontoret delar i huvudsak rekommendationerna men ser också att det är angeläget att informationssäkerheten inte hanteras som ett enskilt arbete utan knyts samman med dataskydd, systemförvaltning, drift, cybersäkerhet samt andra kompetenser inom informationsförvaltning, som exempelvis stadsarkivet. Genom ett integrerat och systematiskt arbetssätt avser staden att nå de effekter som granskningen pekar på och detta arbetssätt har förstärkts och kommer att bli än mer angeläget framåt. Till exempel görs informationsklassningar innan

upphandling av nya system där ovanstående kompetenser deltar tillsammans med den verksamhet som avser att upphandla systemet.

Under 2023 har också ett antal förflyttningar genomförts som adresseras i rapporten. Exempelvis har en ny policy för informationssäkerhet antagits samt en riktlinje för ledningssystem gällande informationssäkerhet. Under året har också en utbildning genomförts för samtliga medarbetare i Västerås stad.

Informationssäkerhet och angränsande områden har blivit alltmer angeläget i takt med ökat beroende till digitala lösningar och ökade risker och hot i omvärlden. Västerås stad behöver, precis som övriga offentliga aktörer, prioritera detta och ha ett nära samarbete i frågorna.

Stadsledningskontoret har till kommunstyrelsen lämnat följande förslag till beslut:

Förslag till kommunfullmäktige:

1. Stadsledningskontorets förslag till yttrande daterat 2024-02-28 antas och lämnas över till Västerås stads revisorer.

2. Revisionsrapporten läggs till handlingarna

Kopia till

Samtliga nämnder

Kommunstyrelsen
Jörgen Sandström
Epost: jorgen.sandstrom@vasteras.se

Kopia till
Samtliga nämnder

Kommunstyrelsen

Tjänsteutlåtande - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Förslag till beslut

Förslag till kommunfullmäktige:

1. Stadsledningskontorets förslag till yttrande daterat 2024-02-28 antas och lämnas över till Västerås stads revisorer.

2. Revisionsrapporten läggs till handlingarna

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation.

Rapporten lämnades till kommunstyrelsen den 9 mars 2023 och har remitterats till samtliga nämnder i staden, vilka sedan inkommit med yttranden.

I granskningen har förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen följande:

• En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

• En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

• En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Västerås stad bedömdes ha en genomsnittlig mognadsgrad på 2,50, vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52.

De remitterade nämnderna och stadsledningskontoret delar i huvudsak rekommendationerna men ser också att det är angeläget att informationssäkerheten inte hanteras som ett enskilt arbete utan knyts samman med dataskydd, systemförvaltning, drift, cybersäkerhet samt andra

kompetenser inom informationsförvaltning, som exempelvis stadsarkivet. Genom ett integrerat och systematiskt arbetssätt avser staden att nå de effekter som granskningen pekar på och detta arbetssätt har förstärkts och kommer att bli än mer angeläget framåt. Till exempel görs informationsklassningar innan upphandling av nya system där ovanstående kompetenser deltar tillsammans med den verksamhet som avser att upphandla systemet.

Under 2023 har också ett antal förflyttningar genomförts som adresseras i rapporten. Exempelvis har en ny policy för informationssäkerhet antagits samt en riktlinje för ledningssystem gällande informationssäkerhet. Under året har också en utbildning genomförts för samtliga medarbetare i Västerås stad.

Informationssäkerhet och angränsande områden har blivit alltmer angeläget i takt med ökat beroende till digitala lösningar och ökade risker och hot i omvärlden. Västerås stad behöver, precis som övriga offentliga aktörer, prioritera detta och ha ett nära samarbete i frågorna.

Stadsledningskontoret har till kommunstyrelsen lämnat följande förslag till beslut:

Förslag till kommunfullmäktige:

1. Stadsledningskontorets förslag till yttrande daterat 2024-02-28 antas och lämnas över till Västerås stads revisorer.

2. Revisionsrapporten läggs till handlingarna

Juridisk bedömning

Kommunstyrelsen är behörig att fatta beslutet i enlighet med kommunstyrelsens reglemente och kommunallagen.

Ekonomisk bedömning

Informationssäkerhet och angränsande områden blir mer angeläget i takt med ökat beroende av digitala lösningar och ökade risker och hot i omvärlden. Det innebär att kostnaderna för att skydda sig och jobba förebyggande med frågorna likväl som att utbilda personalen ökar över tid. Finansieringen hanteras löpande i arbetet med årsplan.

Hållbar utveckling

Att upprätthålla förtroende för att Västerås stad hanterar informationstillgångar är angeläget och en förutsättning för fortsatt digitalisering. En hållbar utveckling har stort stöd av att det sker en fortsatt utveckling av offentliga digitala tjänster.

Helene Öhrling
Stadsdirektör

Jörgen Sandström
Digitaliseringsdirektör

Kommunstyrelsen
Jörgen Sandström
Epost: jorgen.sandstrom@vasteras.se

Kommunstyrelsen

Yttrande - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation.

Rapporten lämnades till kommunstyrelsen den 9 februari 2023 och har remitterats till samtliga nämnder i staden, vilka sedan inkommit med yttranden.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen i Västerås stad att tillse:

• En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

• En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

• En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Revisionen utgick ifrån kriterier som sätts genom Myndigheten för samhällsskydd och beredskaps (MSB) ramverk ledningssystem för informationssäkerhet (LIS), ISO/IEC 27000, Kommunallagen samt stadens gällande och relevanta styrdokument inom IT- och informationssäkerhet

Västerås stad bedömdes ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun som Västerås. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

Samtliga nämnder har yttrat sig angående revisionsrapport 2022:5 om IT- och informationssäkerheten i Västerås stad. Sammanfattningsvis så delar nämnderna i huvudsak rapportens rekommendationer.

Dessutom betonar miljö- och konsumentnämnden vikten av att samordna styrdokumenten med en tydlig struktur för att underlätta för anställda att följa kommunens IT- och informationssäkerhetsarbete samt att nämnder troligen har kommit olika långt i sitt arbete med IT- och informationssäkerhet vilket bör beaktas.

Äldrenämnden ser att det finns brister i det systematiska informationssäkerhetsarbetet men anger även svårigheter att hitta relevant information inom området.

Grundskolennämnden och utbildningsnämnden lyfter fram behovet av ett integrerat ledningssystem som omfattar informationssäkerhet, IT-säkerhet och GDPR samt ett intresse att utforska Mognadsdialog som ett verktyg för att stärka det systematiska informationssäkerhetsarbetet.

Byggnadsnämnden och nämnden för idrott och fritid lyfter fram vikten av ett stadsövergripande och gemensamt arbetssätt och sammanhållen styrning inom området.

Stadsledningskontoret jobbar kontinuerligt med att stödja nämnder och förvaltningar med informationssäkerhet, dataskydd och IT-säkerhet. Det görs i nära samverkan med de som tillhandahåller digitala lösningar för stadens verksamheter. Arbetet innefattar även att styra samt initiera förbättringar i arbetssätt samt föreslå åtgärder som skyddar stadens informationstillgångar.

Informationssäkerheten kan inte hanteras som ett enskilt arbete utan behöver knytas samman med i ett integrerat arbete samman med dataskydd, systemförvaltning, IT-drift, cybersäkerhet, juridik, upphandling samt andra kompetenser inom informationsförvaltning såsom stadsarkiv och registratur.

Med ett integrerat och systematiskt arbetssätt så når man de effekter som granskningen pekar på, vilket också utbildningsnämnden betonar. Det är ett arbetssätt som förstärkts på senare år och kommer att bli än mer angeläget framåt. Till exempel görs informationsklassningar innan upphandling av nya system där ovanstående kompetenser deltar tillsammans med verksamheten som avser upphandla systemet.

Under 2023 genomfördes också en förstudie kring informationsförvaltningsprocesser som samlade merparten av ovan nämnda förmågor som på lång sikt kommer skapa ett proaktivt arbetssätt som hanterar risker och informationsklassning i ett tidigt skede när vi etablerar tjänster och arbetssätt baserat på digital teknik. Inte minst framväxten av maskinlärande och AI har eskalerat behoven av att hantera information rätt och säkert från början.

Redan när granskningen genomfördes hade ett antal aktiviteter påbörjats och planerats som är samstämmiga med granskningens rekommendationer, dessa har sedan fullföljts.

Under våren 2023 antogs en ny informationssäkerhetspolicy samt en riktlinje för ledningssystem för informationssäkerhet och under hösten 2023 en

genomfördes utbildning i informationssäkerhet för samtliga medarbetare i Västerås stad. Dessutom finns ett arbetssätt där man mer integrerat arbetar med dataskydd, IT-säkerhet, informationssäkerhet samt upphandling i samverkan med stadens systemförvaltningar.

Informationssäkerhet och angränsande områden har blivit alltmer angeläget i takt med ökat beroende till digitala lösningar och ökade risker och hot i omvärlden. Västerås stad behöver, precis som övriga offentliga aktörer, prioritera detta och ha ett nära samarbete i frågorna. SKR-koncernen har också på senare tid prioriterat frågorna då det blivit en större utmaning för kommuner och regioner. Deras roll att hålla samman kommunal verksamhet kommer att vara en väsentlig del i framgången, inte minst genom deras kontakter med ansvariga myndigheter på området.

§ 20 Dnr VN 2023/00005-1.7.1

Beslut - Svar på remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Yttrande daterat 2023-04-24 antas och överlämnas till kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats till kommunstyrelsen.

Kommunstyrelsen har i en remiss begärt in yttrande över granskningsrapporten från samtliga nämnder senast den 10 maj. Valnämnden har begärt att få till den 17 maj på sig att svara och det har beviljats.

Valkansliet har till valnämnden lämnat följande förslag till beslut:

Yttrande daterat 2023-04-24 antas och överlämnas till kommunstyrelsen.

Kopia till

Kommunstyrelsen

VÄSTERÅS STAD

YTTRANDE

Datum
2023-04-24

Diarienr
VN 2023/00005- 1.7.1

Valnämndens kansli, Stadsledningskontoret
Sofia Ersson
Epost: sofia.ersson@vasteras.se

Kommunstyrelsen

Yttrande Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Valnämnden har tagit del av granskningsrapporten och dess rekommendationer som revisionen riktat till kommunstyrelsen. Valnämnden följer det fortsatta arbetet som leds av kommunstyrelsen och avser genomföra de aktiviteter som tas fram stadsövergripande.

Vad gäller valnämndens eget ansvarsområde inom it-säkerhet så ligger det endast inom ägandet och förvaltningen av verksamhetssystemet Mobilise. Bedömningen är att Mobilise håller den it-säkerhetsnivå som krävs för den information och de funktioner som systemet innehar. Vid behov görs översyner av säkerhetsnivån i samråd med Västerås stads it-säkerhetsstrateger.

§ 77 Dnr NIF 2023/00050-1.7.1

Beslut-Remiss, Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Nämnden antar förvaltningens förslag till yttrande daterat 2023-04-03 och överlämnar till Kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation. Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, ”Granskningsprogram Cyber- och Informationssäkerhet”, särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 57 punkter på en ordinarie skala från 1 (begynnande) till 5 (optimerad) inom de respektive områdena.

Representanter för kommunens informationssäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Förvaltningen lämnar följande förslag till beslut:

Nämnden antar förvaltningens förslag till yttrande daterat 2023-04-03 och överlämnar till Kommunstyrelsen.

Yrkanden

Vicki Skure Eriksson (C) yrkar bifall till förvaltningen förslag till beslut.

Proposition

Ordföranden finner att det finns ett förslag till beslut och att nämnden beslutar enligt detta.

Kopia till

Kommunstyrelsen

VÄSTERÅS STAD

YTTRANDE

Datum
2023-04-03

Diarienr
NIF 2023/00050- 1.7.1

Kultur-, idrott- och fritidsförvaltningen
Lenny Hallgren
Epost: lenny.hallgren@vasteras.se

Kommunstyrelsen

Yttrande Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Kultur- idrotts- och fritidsförvaltningen anser att revisionsrapporten är bra och tydlig. De förbättringsområden som har identifierats och som EY rekommenderar Kommunstyrelsen att genomföra är alla bra och skulle hjälpa nämnden i sitt arbete i detta komplexa och mycket viktiga område.

Som nämnds i rapporten hanterar staden, och nämnden, stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig samt har tillräckligt starkt skydd.

Nämnden har ett behov av en stark central styrning inom detta område och ser fram emot de åtgärder som kommer att vidtas av Kommunstyrelsen och nämnden kommer att göra allt som krävs för att uppfylla de åtaganden som nämnden har.

§ 72 Dnr TN 2023/00105-1.7.1

Beslut - Yttrande över revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

1. Yttrandet godkänns och överlämnas till kommunstyrelsen.

Ärendebeskrivning

EY har på uppdrag av Västerås stads förtroendevalda revisorer genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet och resultatet visar att Västerås stad har en genomsnittlig mognadsgrad som är något lägre än andra offentliga organisationer av liknande storlek och karaktär. I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

* En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

* En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

* En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Teknik- och fastighetsförvaltningen har i tjänstutlåtande, daterat den 31 mars 2023, lämnat förslag till beslut:

1. Yttrandet godkänns och överlämnas till kommunstyrelsen.

Yrkanden

Karin Westlund (C) yrkar bifall till teknik- och fastighetsförvaltningens förslag till beslut.

Kopia till

Kommunstyrelsen

VÄSTERÅS STAD

YTTRANDE

Datum
2023-03-31

Diarienr
TN 2023/00105- 1.7.1

Teknik- och fastighetsförvaltningen
Emma Rimbe
Epost: emma.rimbe@vasteras.se

Kommunstyrelsen

Yttrande över Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

EY:s främsta rekommendationer är att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete

Tekniska nämnden ställer sig bakom EY:s rekommendationen att en plan bör upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen. Nämnden upplever en avsaknad av tillgängligt ledningssystem som hanterar helheten kopplat till informationssäkerhet och det är svårt att hitta relevant information. Nämnden efterfrågar också en övergripande beskrivning av hur helheten hänger ihop. Upplevelsen idag är att informationssäkerhet inte är integrerad arbetsmässigt med IT-säkerhet och GDPR utan hanteras som separata spår. Nämnden vill se en tydligare samverkan styrningsmässigt inom dessa områden.

Tekniska nämnden ställer sig bakom EY:s rekommendation att det ska finnas en dokumenterad utbildningsplan för samtliga medarbetare som innefattar helheten kopplat till informationssäkerhet. Till nyanställda bör den här delen ingå i ett introduktionspaket.

Tekniska nämnden anser att en heltäckande internkontroll avseende IT- och informationssäkerhet, som är integrerad i stadens övergripande internrevision och kvalitetsarbete, skulle kunna vara ett alternativ.

VÄSTERÅS STAD

TJÄNSTEUTLÅTANDE

Datum
2023-03-31

Diarienr
TN 2023/00105- 1.7.1

Teknik- och fastighetsförvaltningen
Emma Rimbe
Epost: emma.rimbe@vasteras.se

Kopia till
Kommunstyrelsen

Tekniska nämnden

Tjänsteutlåtande - Yttrande över Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Förslag till beslut

1. Yttrandet godkänns och överlämnas till kommunstyrelsen.

Ärendebeskrivning

EY har på uppdrag av Västerås stads förtroendevalda revisorer genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet och resultatet visar att Västerås stad har en genomsnittlig mognadsgrad som är något lägre än andra offentliga organisationer av liknande storlek och karaktär. I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

TEKNIK- OCH FASTIGHETSFÖRVALTNINGEN

Hans Näslund
Direktör

Emma Rimbe
Utvecklingsstrateg

§ 98 Dnr AN 2023/00209-1.6.1

Yttrande till Kommunstyrelsen över remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Äldrenämnden antar vård- och omsorgsförvaltningens förslag till yttrande daterat 14 april 2023 och överlämnar det till kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen i Västerås stad att tillse:

* En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

* En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

* En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Vård- och omsorgsförvaltningen har i sitt förslag till yttrande tagit ställning till EY´s rekommendationer.

Vård- och omsorgsförvaltningen har till äldrenämnden lämnat följande förslag till beslut:

Äldrenämnden antar vård- och omsorgsförvaltningens förslag till yttrande daterat 14 april 2023 och överlämnar det till kommunstyrelsen.

Kopia till

Kommunstyrelsen

VÄSTERÅS STAD

TJÄNSTEUTLÅTANDE

Datum
2023-04-14

Diarienr
AN 2023/00209- 1.6.1

Vård- och omsorgsförvaltningen
Anne Almqvist
Epost: anne.almqvist@vasteras.se

Kopia till
Kommunstyrelsen

Äldrenämnden

Tjänsteutlåtande - Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Förslag till beslut

Äldrenämnden antar vård- och omsorgsförvaltningens förslag till yttrande daterat 14 april 2023 och överlämnar det till kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen i Västerås stad att tillse:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Vård- och omsorgsförvaltningen har i sitt förslag till yttrande tagit ställning till EY´s rekommendationer.

Vård- och omsorgsförvaltningen har till äldrenämnden lämnat följande förslag till beslut:

Äldrenämnden antar vård- och omsorgsförvaltningens förslag till yttrande daterat 14 april 2023 och överlämnar det till kommunstyrelsen.

Vård- och omsorgsförvaltningen
Anne Almqvist
Epost: anne.almqvist@vasteras.se

Kommunstyrelsen, Västerås stad

Yttrande Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

En remiss har inkommit från kommunstyrelsen där äldrenämnden ges möjlighet att yttra sig över revisionsrapport 2022:5 - Granskning av IT- och informationssäker.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen i Västerås stad att tillse:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Äldrenämnden rekommenderar att:

- en plan bör upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom staden och att riktlinjer avseende IT- och informationssäkerhet revideras kontinuerligt utefter ett förutbestämt tidsintervall för att säkerställa att riktlinjer förbli riktiga och aktuella över tid.
  Äldrenämnden saknar ett stöd i form av ett tydligt och tillgängligt ledningssystem som beskriver och samordnar ett systematiskt och riskbaserat informationssäkerhetsarbete och det upplevs svårt att hitta relevant information.

- att det ska finnas en dokumenterad utbildningsplan för samtliga medarbetare för såväl långvariga medarbetare som nyanställda och säkerställa att genomförandet av utbildningar bland medarbetare kontinuerligt följs upp.

Åter igen ställs krav utifrån att staden är leverantör av samhällsviktiga tjänster:

*MSBFS 2018:8**,** 9 § En leverantör ska ha interna regler och arbetssätt som säkerställer att medarbetarna har kunskap om säker hantering av information, genom att:*

1. hålla relevanta interna regler och stöd för säker informationshantering kända för medarbetarna,

2. regelbundet och utifrån identifierat behov och arbetsuppgifter utveckla och upprätthålla medarbetarnas kompetens genom utbildning, informationsinsatser och övning, samt

3. följa upp och utvärdera organisationens förmåga att förmedla kunskap till medarbetarna om säker hantering av information.

- ett arbete med internkontroll som täcker samtliga områden inom stadens IT- och informationssäkerhetsarbete behövs för att veta huruvida det systematiska informationssäkerhetsarbetet, riskhanteringsarbetet och de beslutade säkerhetsåtgärderna är ändamålsenligt utformade, har avsedd verkan, existerar och fungerar tillfredsställande. Resultatet av internkontroller behövs delas med ledningen/ansvariga för att få samsyn gällande det fortsatta arbetet.

Äldrenämndens arbete med IT- och informationssäkerhet

Revisionsrapportens resultat belyser kommunövergripande brister. Äldrenämnden, nedan benämnd nämnden, arbetar genom vård- och omsorgsförvaltningen aktivt och förebyggande med IT- och informationssäkerhet och redovisar detta nedan.

2.1 Nuläge och iakttagelser inom huvudområdet Styrning

Område Ledningssystem
Iakttagelser Kommunen har inte ett uppdaterat och helt fungerande Ledningssystem för informationssäkerhet (LIS).
Nämndens informationssäkerhetsarbete Förvaltningen har påbörjat ett arbete med att införa ett eget ledningssystem för informationssäkerhet. Förvaltningen har som vårdgivare och utifrån lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (Hälso- och sjukvård) krav på att ha ett ledningssystem för informationssäkerhet.

Område Policy
Iakttagelser Den gällande informationssäkerhetspolicyn är mer än 10 år gammal.
Det saknas en dokumenterad process för hur det säkerställs att medarbetare kontinuerligt tar del av policy och riktlinjer avseende IT- och informationssäkerhet.
En dokumenterad process för hur det säkerställs att nyanställda har tagit del av policy och riktlinjer avseende IT- och informationssäkerhet har ännu inte blivit implementerad.

Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Strategi och rutiner
Iakttagelser Det saknas en definierad frekvens för hur ofta riktlinjer avseende informationssäkerhet ska granskas.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Organisation
Iakttagelser Styrdokumenten är till viss del utdaterade.
Det saknas formaliserade kontroller och rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet hos verksamheterna.
Nämndens informationssäkerhetsarbete Objektägaren/objektledare samt dataskyddssamordnare på förvaltningen följer årligen upp arbetet med informationssäkerhet genom internrevisioner, riskanalyser och åtgärdskontroll.

2.2 Nuläge och iakttagelser inom huvudområdet Personal och behörigheter

Område Personal
Iakttagelser Utbildning i informationssäkerhet är inte obligatoriskt.
Det saknas obligatorisk utbildning i informationssäkerhet till nyanställda.
Nämndens informationssäkerhetsarbete Under förra året har förvaltningens medarbetare erbjudits att ta del av en mikroutbildning gällande informationssäkerhet.

Område Behörighetshantering
Iakttagelser Det saknas en dokumenterad process avseende att systemägare ska dokumentera genomförandet av periodisk genomgång av behörigheter.
Kommunen saknar en dokumenterad process för att säkerställa segregering av roller och behörigheter inom organisation och system.
Det finns ingen dokumenterad uppföljning på att lösenordspolicyn följs.
Nämndens informationssäkerhetsarbete Förvaltningen har en dokumenterad process att granska behörigheter varje kvartal.
Förvaltningen har en dokumenterad process för att säkerställa segregering av roller och behörigheter. För anställda inom hälso- och sjukvård ska en individuell behovs- och riskanalys alltid göras före tilldelning av behörighet.
Samtliga verksamhetssystem kräver två-faktorsinloggning och lösenord är inte tillåtet.

2.3 Nuläge och iakttagelser inom huvudområdet Drift

Område Incidenthantering
Iakttagelser Incidenthanterings-processen beskriver inte hur uppföljning av incidenter på aggregerad nivå ska ske.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Informationsklassning
Iakttagelser Västerås stad hänvisar fortfarande till stor del till PuL.
Nämndens informationssäkerhetsarbete IT-systemen klassas alltid utifrån den information som behandlas och lagras och undersöker behovet av konfidentialitet, riktighet och tillgänglighet.
PuB-avtal tecknas utifrån dataskyddsförordningen med leverantörer.

Område Nätverk
Iakttagelser Nätverksdokumentationen är gammal och bör revideras.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Brandväggar
Iakttagelser Det finns ingen upprättad brandväggspolicy, -instruktion eller liknande.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Kontinuitetsplanering
Iakttagelser Det saknas en rutin för att följa upp och testa kontinuitetsplaner.
Nämndens informationssäkerhetsarbete Rutiner för att granska och följa upp kontinuitetsplaner finns framtagna för varje verksamhetssystem. Följs upp årligen.

2.3 Nuläge och iakttagelser inom huvudområdet Programförändringar

Område Förändringshantering
Iakttagelser För vissa system testas förändringar direkt i produktionsmiljön.
Nämndens informationssäkerhetsarbete Rutiner för förändringshantering finns etablerade.
Förvaltningsplaner är framtagna och beslutade för objektens system.
Tester sker inte i produktionsmiljö utan i acceptans- eller testmiljöer.

§ 72 Dnr FN 2023/00041-1.7.1

Beslut - Yttrande över remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Förslag till yttrande daterat 2023-03-30 godkänns och överlämnas till kommunstyrelsen.

Ärendebeskrivning

EY har på uppdrag av Västerås stads förtroendevalda revisorer genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet och resultatet visar att Västerås stad har en genomsnittlig mognadsgrad som är något lägre än andra offentliga organisationer av liknande storlek och karaktär. I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

* En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

* En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

* En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Teknik- och fastighetsförvaltningen har lämnat följande förslag till beslut:

Förslag till yttrande daterat 2023-03-30 godkänns och överlämnas till kommunstyrelsen.

Yrkanden

Ordföranden yrkar bifall till förvaltningens förslag till beslut.

Kopia till

Kommunstyrelsen

VÄSTERÅS STAD

YTTRANDE

Datum
2023-03-31

Diarienr
FN 2023/00041- 1.7.1

Teknik- och fastighetsförvaltningen
Emma Rimbe
Epost: emma.rimbe@vasteras.se

Kommunstyrelsen

Yttrande Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

EY:s främsta rekommendationer är att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete

Förvaltningen ställer sig bakom EY:s rekommendationen att en plan bör upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen. Förvaltningen upplever en avsaknad av tillgängligt ledningssystem som hanterar helheten kopplat till informationssäkerhet och det är svårt att hitta relevant information. Förvaltningen efterfrågar också en övergripande beskrivning av hur helheten hänger ihop. Upplevelsen idag är att informationssäkerhet inte är integrerad arbetsmässigt med IT-säkerhet och GDPR utan hanteras som separata spår. Förvaltningen vill se en tydligare samverkan styrningsmässigt inom dessa områden.

Förvaltningen ställer sig bakom EY:s rekommendation att det ska finnas en dokumenterad utbildningsplan för samtliga medarbetare som innefattar helheten kopplat till informationssäkerhet. Till nyanställda bör den här delen ingå i ett introduktionspaket.

Förvaltningen anser att en heltäckande internkontroll avseende IT- och informationssäkerhet, som är integrerad i stadens övergripande internrevision och kvalitetsarbete, skulle kunna vara ett alternativ.

§ 93 Dnr GSN 2023/00418-1.7.1

Yttrande till kommunstyrelsen över remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Grundskolenämnden antar barn- och utbildningsförvaltningens yttrande, daterat 2023-03-24, som sitt eget och översänder det till kommunstyrelsen.

Ärendebeskrivning

Kommunstyrelsen har översänt revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet till bland annat grundskolenämnden för yttrande. Yttrandet ska vara kommunstyrelsen tillhanda senast den 10 maj 2023.

EYs granskning har bedömt om kommunens interna kontroll avseende IT- och informationssäkerhet är tillräcklig och i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. De pedagogiska nämnderna har granskats.

Grundskolenämndens yttrande gäller EY:s främsta rekommendationer till kommunstyrelsen i Västerås stad som omfattar även arbete inom grundskolenämnden.

Yrkanden

Jonas Cronert (S) yrkar bifall till förvaltningens förslag till beslut.

Proposition

Ordföranden finner att det finns ett förslag till beslut, förvaltningens förslag till beslut med bifall från ordföranden själv, och att grundskolenämnden beslutar enligt det.

Kopia till

Kommunstyrelsen

VÄSTERÅS STAD

YTTRANDE

Datum
2023-03-24

Diarienr
GSN 2023/00418- 1.7.1

Barn- och Utbildningsförvaltning
Johanna Andersson
Epost: Johanna6.andersson@vasteras.se

Grundskolenämnden

Yttrande Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Inledning

EY:s främsta rekommendationer är att kommunstyrelsen i Västerås stad tillser att:

A. En plan upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

B. En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

C. En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete

Rekommendation A

Nämnden ställer sig bakom EY:s rekommendationen att en plan bör upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen. Nämnden upplever en avsaknad av tillgängligt ledningssystem som hanterar helheten kopplat till informationssäkerhet och det är svårt att hitta relevant information. Nämnden efterfrågar också en övergripande beskrivning av hur helheten hänger ihop. Upplevelsen idag är att informationssäkerhet inte är integrerad arbetsmässigt med IT-säkerhet och GDPR utan hanteras som separata spår. Nämnden vill se en tydligare samverka styrningsmässigt inom dessa områden.

Rekommendation B

Nämnden ställer sig bakom EY:s rekommendationen att det ska finnas en dokumenterad utbildningsplan för samtliga medarbetare som innefattar helheten kopplat till informationssäkerhet. Till nyanställda bör den här delen ingå i ett introduktionspaket.

Rekommendation C

Nämnden anser att en heltäckande internkontroll avseende IT- och informationssäkerhet, som är integrerad i stadens övergripande internrevision, skulle kunna vara ett alternativ. Nämnden önskar dock att kommunstyrelsen tillser att utreda införande av Mognadsdialog kopplat till informationssäkerhet med syfte att undersöka om dialogen skulle kunna ersätta alternativt komplettera internkontrollen.

Mognadsdialogen är framtagen av MSB (Myndigheten för samhällsskydd och beredskap) och är ett pedagogiskt verktyg för uppföljning av organisationens systematiska informationssäkerhetsarbete. Genom dialog skapas förståelse och samsyn om organisationens nuläge och vägen framåt. Det skapar ökat engagemang och möjligheter för ledning och säkerhetsansvariga att tillsammans ”göra rätt saker på rätt sätt”. Dialog och bedömningar utgår *från arbetssätt, tillgänglighet, resultat och uppföljning och lära och förbättra* och hanterar följande perspektiv *riskhantering, informationsklassning, incidenthantering, upphandling, kompetens och upphandling.*

§ 110 Dnr IFN 2023/00094-1.7.1

Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Individ- och familjenämnden antar yttrandet som sitt eget och överlämnar det till Kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Västerås stad bedöms ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Utifrån den mängd personuppgifter och personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden lägre än vad EY rekommenderar för en kommun likt Västerås stad.

Granskningen har identifierat ett antal förbättringsområden och rekommendationer för Västerås stads fortsatta arbete inom området:

* En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

* En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

* En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Inga nämndspecifika rekommendationer har redovisats.

Yrkanden

Ordföranden yrkar bifall till förvaltningens förslag till beslut.

Kopia till

Kommunstyrelsen, Västerås stad

VÄSTERÅS STAD

TJÄNSTEUTLÅTANDE

Datum
2023-04-14

Diarienr
IFN 2023/00094- 1.7.1

Individ- och familjeförvaltningen
Fredrik Lindell
Epost: fredrik.lindell@vasteras.se

Kopia till
Kommunstyrelsen, Västerås stad

Individ- och familjenämnden

Tjänsteutlåtande - Yttrande över Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Förslag till beslut

Individ- och familjenämnden antar yttrandet som sitt eget och överlämnar det till Kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

VÄSTERÅS STAD

Individ och familjeförvaltning
Fredrik Lindell

Dnr: IFN 2023/00094-1.7.1

Yttrande över Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Västerås stad bedöms ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Utifrån den mängd personuppgifter och personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden lägre än vad EY rekommenderar för en kommun likt Västerås stad.

Granskningen har identifierat ett antal förbättringsområden och rekommendationer för Västerås stads fortsatta arbete inom området:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Individ- och familjenämnden delar och bekräftar granskningens rekommendationer och ser att behovet av kunskap och kännedom om informationssäkerhet behövs stärkas i förvaltningen. Nämndens verksamheter har gott stöd med informationssäkerhetresurser i staden. Framför allt när det gäller upphandling, klassning av nya system samt även när det gäller dataskydd.

§ 106 Dnr NF 2023/00066-1.6.1

Yttrande till Kommunstyrelsen över remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Nämnden för personer med funktionsnedsättning antar vård- och omsorgsförvaltningens förslag till yttrande daterat 12 april 2023 och överlämnar det till kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen i Västerås stad att tillse:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Vård- och omsorgsförvaltningen har i sitt förslag till yttrande tagit ställning till EY´s rekommendationer.

Vård- och omsorgsförvaltningen har till nämnden för personer med funktionsnedsättning lämnat följande förslag till beslut:

Nämnden för personer med funktionsnedsättning antar vård- och omsorgsförvaltningens förslag till yttrande daterat 12 april 2023 och överlämnar det till kommunstyrelsen.

Kopia till

Kommunstyrelsen, Västerås stad

VÄSTERÅS STAD

YTTRANDE

Datum
2023-04-12

Diarienr
NF 2023/00066- 1.6.1

Vård- och omsorgsförvaltningen
Anne Almqvist
Epost: anne.almqvist@vasteras.se

Kommunstyrelsen, Västerås stad

Yttrande Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

En remiss har inkommit från kommunstyrelsen där nämnden för personer med funktionsnedsättning ges möjlighet att yttra sig över revisionsrapport 2022:5 - Granskning av IT- och informationssäker.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY har rekommenderat kommunstyrelsen i Västerås stad att tillse:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Nämnden för personer med funktionsnedsättning rekommenderar att:

- en plan bör upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom staden och att riktlinjer avseende IT- och informationssäkerhet revideras kontinuerligt utefter ett förutbestämt tidsintervall för att säkerställa att riktlinjer förbli riktiga och aktuella över tid.
  Nämnden för personer med funktionsnedsättning saknar ett stöd i form av ett tydligt och tillgängligt ledningssystem som beskriver och samordnar ett systematiskt och riskbaserat informationssäkerhetsarbete och det upplevs svårt att hitta relevant information.

- att det ska finnas en dokumenterad utbildningsplan för samtliga medarbetare för såväl långvariga medarbetare som nyanställda och säkerställa att genomförandet av utbildningar bland medarbetare kontinuerligt följs upp.

Åter igen ställs krav utifrån att staden är leverantör av samhällsviktiga tjänster:

*MSBFS 2018:8**,** 9 § En leverantör ska ha interna regler och arbetssätt som säkerställer att medarbetarna har kunskap om säker hantering av information, genom att:*

1. hålla relevanta interna regler och stöd för säker informationshantering kända för medarbetarna,

2. regelbundet och utifrån identifierat behov och arbetsuppgifter utveckla och upprätthålla medarbetarnas kompetens genom utbildning, informationsinsatser och övning, samt

3. följa upp och utvärdera organisationens förmåga att förmedla kunskap till medarbetarna om säker hantering av information.

- ett arbete med internkontroll som täcker samtliga områden inom stadens IT- och informationssäkerhetsarbete behövs för att veta huruvida det systematiska informationssäkerhetsarbetet, riskhanteringsarbetet och de beslutade säkerhetsåtgärderna är ändamålsenligt utformade, har avsedd verkan, existerar och fungerar tillfredsställande. Resultatet av internkontroller behövs delas med ledningen/ansvariga för att få samsyn gällande det fortsatta arbetet.

Nämnden för personer med funktionsnedsättnings arbete med IT- och informationssäkerhet

Revisionsrapportens resultat belyser kommunövergripande brister. Nämnden för personer med funktionsnedsättning, nedan benämnd nämnden arbetar genom vård- och omsorgsförvaltningen aktivt och förebyggande med IT- och informationssäkerhet och redovisar detta nedan.

2.1 Nuläge och iakttagelser inom huvudområdet Styrning

Område Ledningssystem
Iakttagelser Kommunen har inte ett uppdaterat och helt fungerande Ledningssystem för informationssäkerhet (LIS).
Nämndens informationssäkerhetsarbete Förvaltningen har påbörjat ett arbete med att införa ett eget ledningssystem för informationssäkerhet. Förvaltningen har som vårdgivare och utifrån lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (Hälso- och sjukvård) krav på att ha ett ledningssystem för informationssäkerhet.

Område Policy
Iakttagelser Den gällande informationssäkerhetspolicyn är mer än 10 år gammal.
Det saknas en dokumenterad process för hur det säkerställs att medarbetare kontinuerligt tar del av policy och riktlinjer avseende IT- och informationssäkerhet.

En dokumenterad process för hur det säkerställs att nyanställda har tagit del av policy och riktlinjer avseende IT- och informationssäkerhet har ännu inte blivit implementerad.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Strategi och rutiner
Iakttagelser Det saknas en definierad frekvens för hur ofta riktlinjer avseende informationssäkerhet ska granskas.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Organisation
Iakttagelser Styrdokumenten är till viss del utdaterade.
Det saknas formaliserade kontroller och rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet hos verksamheterna.
Nämndens informationssäkerhetsarbete Objektägaren/objektledare samt dataskyddssamordnare på förvaltningen följer årligen upp arbetet med informationssäkerhet genom internrevisioner, riskanalyser och åtgärdskontroll.

2.2 Nuläge och iakttagelser inom huvudområdet Personal och behörigheter

Område Personal
Iakttagelser Utbildning i informationssäkerhet är inte obligatoriskt.
Det saknas obligatorisk utbildning i informationssäkerhet till nyanställda.
Nämndens informationssäkerhetsarbete Under förra året har förvaltningens medarbetare erbjudits att ta del av en mikroutbildning gällande informationssäkerhet.

Område Behörighetshantering
Iakttagelser Det saknas en dokumenterad process avseende att systemägare ska dokumentera genomförandet av periodisk genomgång av behörigheter.
Kommunen saknar en dokumenterad process för att säkerställa segregering av roller och behörigheter inom organisation och system.
Det finns ingen dokumenterad uppföljning på att lösenordspolicyn följs.
Nämndens informationssäkerhetsarbete Förvaltningen har en dokumenterad process att granska behörigheter varje kvartal.
Förvaltningen har en dokumenterad process för att säkerställa segregering av roller och behörigheter. För anställda inom hälso- och sjukvård ska en individuell behovs- och riskanalys alltid göras före tilldelning av behörighet.
Samtliga verksamhetssystem kräver två-faktorsinloggning och lösenord är inte tillåtet.

2.3 Nuläge och iakttagelser inom huvudområdet Drift

Område Incidenthantering
Iakttagelser Incidenthanterings-processen beskriver inte hur uppföljning av incidenter på aggregerad nivå ska ske.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Informationsklassning
Iakttagelser Västerås stad hänvisar fortfarande till stor del till PuL.
Nämndens informationssäkerhetsarbete IT-systemen klassas alltid utifrån den information som behandlas och lagras och undersöker behovet av konfidentialitet, riktighet och tillgänglighet.
PuB-avtal tecknas utifrån dataskyddsförordningen med leverantörer.

Område Nätverk
Iakttagelser Nätverksdokumentationen är gammal och bör revideras.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Brandväggar
Iakttagelser Det finns ingen upprättad brandväggspolicy, -instruktion eller liknande.
Nämndens informationssäkerhetsarbete Stadsgemensamt behov

Område Kontinuitetsplanering
Iakttagelser Det saknas en rutin för att följa upp och testa kontinuitetsplaner.
Nämndens informationssäkerhetsarbete Rutiner för att granska och följa upp kontinuitetsplaner finns framtagna för varje verksamhetssystem. Följs upp årligen.

2.3 Nuläge och iakttagelser inom huvudområdet Programförändringar

Område Förändringshantering
Iakttagelser För vissa system testas förändringar direkt i produktionsmiljön.
Nämndens informationssäkerhetsarbete Rutiner för förändringshantering finns etablerade.
Förvaltningsplaner är framtagna och beslutade för objektens system.
Tester sker inte i produktionsmiljö utan i acceptans- eller testmiljöer.

§ 60 Dnr MOKN 2023/00027-1.7.1

Remiss – Revisionsrapport 2022:5 – Granskning av IT- och informationssäkerhet

Beslut

Förslag till yttrande godkänns och överlämnas till kommunstyrelsen.

Ärendebeskrivning

Kommunstyrelsen har remitterat EY:s revisionsrapport till samtliga nämnder i Västerås stad. Nämndernas yttrande ska vara inskickade till kommunstyrelsen senast den 10 maj 2023 (dnr: KS 2022/00929).

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Miljö- och hälsoskyddsförvaltningen har till miljö- och konsumentnämnden lämnat följande förslag till beslut:

Förslag till yttrande godkänns och överlämnas till kommunstyrelsen.

Proposition

Ordföranden finner att det finns ett förslag till beslut och att nämnden beslutar enligt detta.

Kopia till

Kommunstyrelsen
kommunstyrelsen@vasteras.se

VÄSTERÅS STAD

TJÄNSTEUTLÅTANDE

Datum
2023-04-03

Diarienr
MOKN 2023/00027- 1.7.1

Miljö- och hälsoskyddsförvaltningen
Marianne Lidman Hägnesten
Epost: marianne.lidman.hagnesten@vasteras.se

Miljö- och konsumentnämnden

Kopia till
Kommunstyrelsen
kommunstyrelsen@vasteras.se

Revisionsrapport 2022:5 – Granskning av IT- och informationssäkerhet

Förslag till beslut

Förslag till yttrande godkänns och överlämnas till kommunstyrelsen.

Ärendebeskrivning

Kommunstyrelsen har remitterat EY:s revisionsrapport till samtliga nämnder i Västerås stad. Nämndernas yttrande ska vara inskickade till kommunstyrelsen senast den 10 maj 2023 (dnr: KS 2022/00929).

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Miljö- och hälsoskyddsförvaltningen har till miljö- och konsumentnämnden lämnat följande förslag till beslut:

Förslag till yttrande godkänns och överlämnas till kommunstyrelsen.

Underlag

- Yttrande – Revisionsrapport 2022:5 – Granskning av IT- och informationssäkerhet
- Revisionsrapport 2022:5 – Granskning IT- och informationssäkerhet, december 2022

VÄSTERÅS STAD

YTTRANDE

Datum
2023-04-03

Diarienr
MOKN 2023/00027- 1.7.1

Miljö- och hälsoskyddsförvaltningen
Marianne Lidman Hägnesten
Epost: marianne.lidman.hagnesten@vasteras.se

Kommunstyrelsen

Revisionsrapport 2022:5 – Granskning av IT- och informationssäkerhet

Inledning

Utifrån genomförd revision rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informations-säkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Synpunkter

Nämnden kan konstatera att det finns en mängd beslutade styrdokument i staden, även inom IT- och informationssäkerhetsområdet. Det vore önskvärt att styrdokumenten samordnas med en tydlig struktur så att det blir lättare för kommunens anställda att följa kommunens IT- och informations-säkerhetsarbete. Det kan bland annat vara svårt att förstå hur detta arbete hänger ihop med informationssäkerhet utifrån dataskyddsförordningen.

Nämnden ställer sig bakom EY:s rekommendation om att det ska finnas en gemensam utbildningsplan för samtliga medarbetare. Det bör vara enkelt att följa upp vilka utbildningsinsatser som en medarbetare har genomfört.

Vad gäller rekommendationen om att upprätta en internkontrollplan kan nämnden konstatera att de olika nämnderna troligen har kommit olika långt i sitt arbete kring IT- och informationssäkerhet. I samband med att miljö- och konsumentnämnden upphandlade ett nytt verksamhetssystem 2019 har ett omfattande arbete kring IT-säkerhet påbörjats.

§ 93

Dnr UTN 2023/00125-1.7.1

Yttrande till kommunstyrelsen över remiss avseende revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Utbildningsnämnden antar barn- och utbildningsförvaltningens yttrande, daterat 2023-03-24, som sitt eget och översänder det till kommunstyrelsen.

Ärendebeskrivning

Kommunstyrelsen har översänt revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet till bland annat grundskolenämnden för yttrande. Yttrandet ska vara kommunstyrelsen tillhanda senast den 10 maj 2023.

EYs granskning har bedömt om kommunens interna kontroll avseende IT- och informationssäkerhet är tillräcklig och i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. De pedagogiska nämnderna har granskats.

Utbildningsnämndens yttrade gäller EY:s främsta rekommendationer till kommunstyrelsen i Västerås stad som omfattar även arbete inom utbildningsnämnden.

Yrkanden

Eva-Lotta Svensson (C) yrkar bifall till förvaltningens förslag till beslut.

Proposition

Ordförande finner att det finns ett förslag till beslut, förvaltningens förslag till beslut med bifall från ordförande själv, och att utbildningsnämnden beslutar enligt det.

Kopia till

Kommunstyrelsen

Barn och Utbildningsförvaltning
Handläggare: Johanna Andersson
Epost: Johanna6.andersson@vasteras.se

Utbildningsnämnden

Yttrande till kommunstyrelsen av revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Inledning

EY:s främsta rekommendationer är att kommunstyrelsen i Västerås stad tillser att:

A. En plan upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

B. En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

C. En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete

Rekommendation A

Nämnden ställer sig bakom EY:s rekommendationen att en plan bör upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen. Nämnden upplever en avsaknad av tillgängligt ledningssystem som hanterar helheten kopplat till informationssäkerhet och det är svårt att hitta relevant information. Nämnden efterfrågar också en övergripande beskrivning av hur helheten hänger ihop. Upplevelsen idag är att informationssäkerhet inte är integrerad arbetsmässigt med IT-säkerhet och GDPR utan hanteras som separata spår. Nämnden vill se en tydligare samverka styrningsmässigt inom dessa områden.

Rekommendation B

Nämnden ställer sig bakom EY:s rekommendationen att det ska finnas en dokumenterad utbildningsplan för samtliga medarbetare som innefattar helheten kopplat till informationssäkerhet. Till nyanställda bör den här delen ingå i ett introduktionspaket.

Rekommendation C

Nämnden anser att en heltäckande internkontroll avseende IT- och informationssäkerhet, som är integrerad i stadens övergripande internrevision, skulle kunna vara ett alternativ. Nämnden önskar dock att kommunstyrelsen tillser att utreda införande av Mognadsdialog kopplat till informationssäkerhet med syfte att undersöka om dialogen skulle kunna ersätta alternativt komplettera internkontrollen.

Mognadsdialogen är framtagen av MSB (Myndigheten för samhällsskydd och beredskap) och är ett pedagogiskt verktyg för uppföljning av organisationens systematiska informationssäkerhetsarbete. Genom dialog skapas förståelse och samsyn om organisationens nuläge och vägen framåt. Det skapar ökat engagemang och möjligheter för ledning och säkerhetsansvariga att tillsammans ”göra rätt saker på rätt sätt”. Dialog och bedömningar utgår *från arbetssätt, tillgänglighet, resultat och uppföljning och lära och förbättra* och hanterar följande perspektiv *riskhantering, informationsklassning, incidenthantering, upphandling, kompetens och upphandling.*

§ 70 Dnr KDNS 2023/00123-1.7.1

Remissyttrande - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet (svar klart senast 230512)

Beslut

Kommundelsnämnden har tagit del av revisionsrapport 2022:5 Granskning av IT- och informationssäkerhet och har ingen synpunkt på rapporten.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten. Följande revisionskriterier användes: ? Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk ledningssystem för informationssäkerhet (LIS), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000. ? Kommunallagen ? Stadens gällande och relevanta styrdokument inom IT- och informationssäkerhet Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

Kopia till

Kommunstyrelsen

Kommunrevisionen

VÄSTERÅS STAD

TJÄNSTEUTLÅTANDE

Datum
2023-03-09

Diarienr
KDNS 2023/00123- 1.7.1

Skultuna kommundelsnämnd
Rasmus Persson
Epost: rasmus.persson@vasteras.se

Skultuna kommundelsnämnd

Kopia till
Kommunstyrelsen Västerås stad
Kommunrevisionen Västerås stad

Tjänsteutlåtande - Revisionsrapport 2022:5 Granskning av IT- och informationssäkerhet

Förslag till beslut

Skultuna kommundelsnämnd har tagit del av revisionsrapport 2022:5 Granskning av IT- och informationssäkerhet och har inget att erinra till rapporten.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten. Följande revisionskriterier användes: ► Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk ledningssystem för informationssäkerhet (LIS), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000. ► Kommunallagen ► Stadens gällande och relevanta styrdokument inom IT- och informationssäkerhet Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

§ 92 Dnr FSN 2023/00095-1.7.1

Yttrande till kommunstyrelsen över remiss gällande revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Förskolenämnden antar barn- och utbildningsförvaltningens yttrande, daterat 2023-03-24, som sitt eget och översänder det till kommunstyrelsen.

Ärendebeskrivning

Kommunstyrelsen har översänt revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet till bland annat grundskolenämnden för yttrande. Yttrandet ska vara kommunstyrelsen tillhanda senast den 10 maj 2023.

EYs granskning har bedömt om kommunens interna kontroll avseende IT- och informationssäkerhet är tillräcklig och i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. De pedagogiska nämnderna har granskats.

Förskolenämndens yttrade gäller EY:s främsta rekommendationer till kommunstyrelsen i Västerås stad som omfattar även arbete inom förskolenämnden.

Yrkanden

Solveig Nilsson (S) yrkar bifall till förvaltningens förslag till beslut.

Proposition

Ordförande finner att det finns ett förslag till beslut, förvaltningens förslag till beslut med bifall från ordförande själv, och att förskolenämnden beslutar enligt det.

Kopia till

Kommunstyrelsen

Barn och Utbildningsförvaltning
Handläggare: Johanna Andersson
Epost: Johanna6.andersson@vasteras.se

Förskolenämnden

Yttrande till kommunstyrelsen av revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Inledning

EY:s främsta rekommendationer är att kommunstyrelsen i Västerås stad tillser att:

A. En plan upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

B. En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

C. En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete

Rekommendation A

Nämnden ställer sig bakom EY:s rekommendationen att en plan bör upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen. Nämnden upplever en avsaknad av tillgängligt ledningssystem som hanterar helheten kopplat till informationssäkerhet och det är svårt att hitta relevant information. Nämnden efterfrågar också en övergripande beskrivning av hur helheten hänger ihop. Upplevelsen idag är att informationssäkerhet inte är integrerad arbetsmässigt med IT-säkerhet och GDPR utan hanteras som separata spår. Nämnden vill se en tydligare samverka styrningsmässigt inom dessa områden.

Rekommendation B

Nämnden ställer sig bakom EY:s rekommendationen att det ska finnas en dokumenterad utbildningsplan för samtliga medarbetare som innefattar helheten kopplat till informationssäkerhet. Till nyanställda bör den här delen ingå i ett introduktionspaket.

Rekommendation C

Nämnden anser att en heltäckande internkontroll avseende IT- och informationssäkerhet, som är integrerad i stadens övergripande internrevision, skulle kunna vara ett alternativ. Nämnden önskar dock att kommunstyrelsen tillser att utreda införande av Mognadsdialog kopplat till informationssäkerhet med syfte att undersöka om dialogen skulle kunna ersätta alternativt komplettera internkontrollen.

Mognadsdialogen är framtagen av MSB (Myndigheten för samhällsskydd och beredskap) och är ett pedagogiskt verktyg för uppföljning av organisationens systematiska informationssäkerhetsarbete. Genom dialog skapas förståelse och samsyn om organisationens nuläge och vägen framåt. Det skapar ökat engagemang och möjligheter för ledning och säkerhetsansvariga att tillsammans ”göra rätt saker på rätt sätt”. Dialog och bedömningar utgår *från arbetssätt, tillgänglighet, resultat och uppföljning och lära och förbättra* och hanterar följande perspektiv *riskhantering, informationsklassning, incidenthantering, upphandling, kompetens och upphandling.*

§ 53 Dnr AMN 2023/00053-1.2.3

Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Beslut

Arbetsmarknadsnämnden antar yttrandet som sitt eget och överlämnar det till kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Västerås stad bedöms ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Utifrån den mängd personuppgifter och personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden lägre än vad EY rekommenderar för en kommun likt Västerås stad.

Granskningen har identifierat ett antal förbättringsområden och rekommendationer för Västerås stads fortsatta arbete inom området:

* En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.

* En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.

* En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Inga nämndspecifika rekommendationer har redovisats.

Kopia till

Kommunstyrelsen

VÄSTERÅS STAD

TJÄNSTEUTLÅTANDE

Datum
2023-04-17

Diarienr
AMN 2023/00053- 1.2.3

Individ- och familjeförvaltningen
Fredrik Lindell
Epost: fredrik.lindell@vasteras.se

Kopia till
Kommunstyrelsen

Arbetsmarknadsnämnden

Tjänsteutlåtande - Remiss - Revisionsrapport 2022:5 - Granskning av IT- och informationssäkerhet

Förslag till beslut

Arbetsmarknadsnämnden antar yttrandet som sitt eget och överlämnar det till kommunstyrelsen.

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Västerås stad bedöms ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Utifrån den mängd personuppgifter och personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden lägre än vad EY rekommenderar för en kommun likt Västerås stad.

Granskningen har identifierat ett antal förbättringsområden och rekommendationer för Västerås stads fortsatta arbete inom området:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Inga nämndspecifika rekommendationer har redovisats.

§ 83 Dnr BN 2023/00091-1.7.1

Remiss - Revisionsrapport 2022:5, Granskning av IT- och informationssäkerhet

Beslut

1. Yttrandet över revisionsrapporten godkänns och överlämnas till kommunstyrelsen och Västerås stads revisorer

Ärendebeskrivning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Byggnadsnämnden har ombetts att yttra sig över revisionsrapporten.

I rapporten finns inga direkta rekommendationer till byggnadsnämnden utan verksamheten kommer att påverkas i det kommande stadsövergripande arbetet. Stadsbyggnadsförvaltningen lämnar därför revisionsrapporten utan vidare kommentarer.

Stadsbyggnadsförvaltningen har till byggnadsnämnden lämnat följande förslag till beslut:
1. Yttrandet över revisionsrapporten godkänns och överlämnas till kommunstyrelsen och Västerås stads revisorer

Proposition

Ordföranden finner att det finns ett förslag till beslut och byggnadsnämnden beslutar enligt detta.

VÄSTERÅS STAD

YTTRANDE

Datum
2023-03-06

Diarienr
BN 2023/00091- 1.7.1

Stadsbyggnadsförvaltningen
Anna Mirkovic
Epost: anna.mirkovic@vasteras.se

Kommunstyrelsen

Yttrande Remiss - Revisionsrapport 2022:5, Granskning av IT- och informationssäkerhet

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Byggnadsnämnden har ombetts att yttra sig över revisionsrapporten.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

I rapporten finns inga direkta rekommendationer till byggnadsnämnden utan verksamheten kommer att påverkas i det kommande stadsövergripande arbetet. Stadsbyggnadsförvaltningen lämnar därför revisionsrapporten utan vidare kommentarer.

Västerås stad

Granskning IT- och informationssäkerhet
December 2022

Sammanfattning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Följande revisionskriterier användes:

- Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk ledningssystem för informationssäkerhet (LIS), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.
- Kommunallagen
- Stadens gällande och relevanta styrdokument inom IT- och informationssäkerhet

Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation. Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, "Granskningsprogram Cyber- och Informationssäkerhet" (GCI), särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 57 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive områdena. Representanter för kommunens informationssäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Innehållsförteckning

1 Bakgrund

Västerås stad och dess nämnder hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig samt har tillräckligt starkt skydd.

Under 2020 genomfördes en granskning av följsamheten till dataskyddsförordningen GDPR inom staden, där ett antal väsentliga noteringar gjordes. Sedan dess har den generella hotbilden både inom IT i allmänhet och mot offentliga institutioner i synnerhet ökat. Med utgångspunkt i sin årliga riskanalys 2022 har stadens förtroendevalda revisorer identifierat risker relaterat till kommunens övergripande arbete med informationssäkerhet samt IT-risker.

1.1 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunens interna kontroll avseende IT- och informationssäkerhet är tillräcklig. Vidare är syftet också att bedöma i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande frågor:

- Bedriver Västerås stad ett tillräckligt och ändamålsenligt IT- och informationssäkerhetsarbete?
  - Kan *styrningen* av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?
  - Är arbetet med att *följa upp* att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?
  - Är Västerås stads *incidenthanteringsprocess* ändamålsenlig?
  - Har tillräckliga åtgärder vidtagits av staden med anledning av de rekommendationer som revisionen lämnade vid sin granskning av stadens arbete med GDPR?

1.2 Avgränsning

Granskningen är avgränsad till att ge en övergripande bild av stadens arbete när det gäller IT- och informationssäkerhetsarbetet. Härutöver inkluderar granskningen en uppföljning av den GDPR-granskning som genomfördes av revisorerna 2020. Granskningen omfattar kommunens samtliga nämnder, med kommunstyrelsen som ansvarig nämnd. De kommunala bolagen ingår inte i granskningen.

Granskningen innebär inte att några stickprov, penetrationstester eller dylikt av IT-system genomförs.

1.3 Revisionskriterier

- Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk ledningssystem för informationssäkerhet (LIS), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.
- Kommunallagen
- Stadens gällande och relevanta styrdokument inom IT- och informationssäkerhet

1.4 Metod och genomförande

Granskningen har byggt på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor. Ramverket omfattar flera områden vilka täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i IT- och informationssäkerhet.

Inledningsvis har relevant dokumentation kring kommunens rutiner och processer granskats av EY. Därefter har granskningsmöten hållits med kommunens representanter för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av IT- och informationssäkerhet i kommuner. Under granskningen har dock inga stickprovstester utförts, vilket innebär att själva efterlevnaden av kommunens rutiner och kontroller inte har testats. Slutligen har den samlade bilden av dokumentation samt information inhämtad via granskningsmöten analyserats och bedömts.

Under granskningen har följande roller intervjuats:

- Verksamhetschef
- Tillförordnad projektledare inom digitalisering
- Informationssäkerhetsstrateg
- Säkerhetschef
- Dataskyddsombud

De intervjuade personerna har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

Fullständig källförteckning framgår av bilaga 1.

Under uppdraget har EY granskat 5 huvudområden som brutits ner på 18 underområden enligt nedan.

<u>Styrning</u>

- Ledningssystem
- Policy
- Strategi och rutiner
- Organisation

<u>Personal och behörigheter</u>

- Personal
- Behörighetshantering

Drift

- Incidenthantering
- Informationsklassning
- Nätverk
- Brandväggar
- Kontinuitetsplanering

Programförändringar

- Förändringshantering

Personuppgifter

- Personuppgiftsstyrning
- Personuppgiftsbehandling
- Personuppgiftsrutiner
- Dataskydd
- Utbildning inom dataskyddsförordningen
- Molntjänster

Under granskningen har EY gjort en sammanfattande betygsättning på samtliga 18 underområden på en skala 1–5. Skalans definition presenteras nedan:

Tabell 1: Skala för bedömning av Västerås stadmognadsgrad inom informationssäkerhetsområden

1	Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc
2	Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning
3	Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen
4	Förutom väldokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning
5	Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan till exempel ett område med grön färgkod ändå sakna viktiga delar. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

Tidsplanen för arbetet såg ut enligt följande:

Tabell 2: Tidsplan för IT- och informationssäkerhetsgranskningen

Förberedelser och planering	September 2022
Insamling och analys av dokumentation	Oktober 2022
Arbetsmöte	Oktober 2022
Rapportskrivning samt intern kvalitetssäkring	Oktober 2022
Faktagranskning av kommunen	November 2022
Justering samt färdigställande av rapport	November 2022
Avrapportering och slutpresentation	Januari 2023

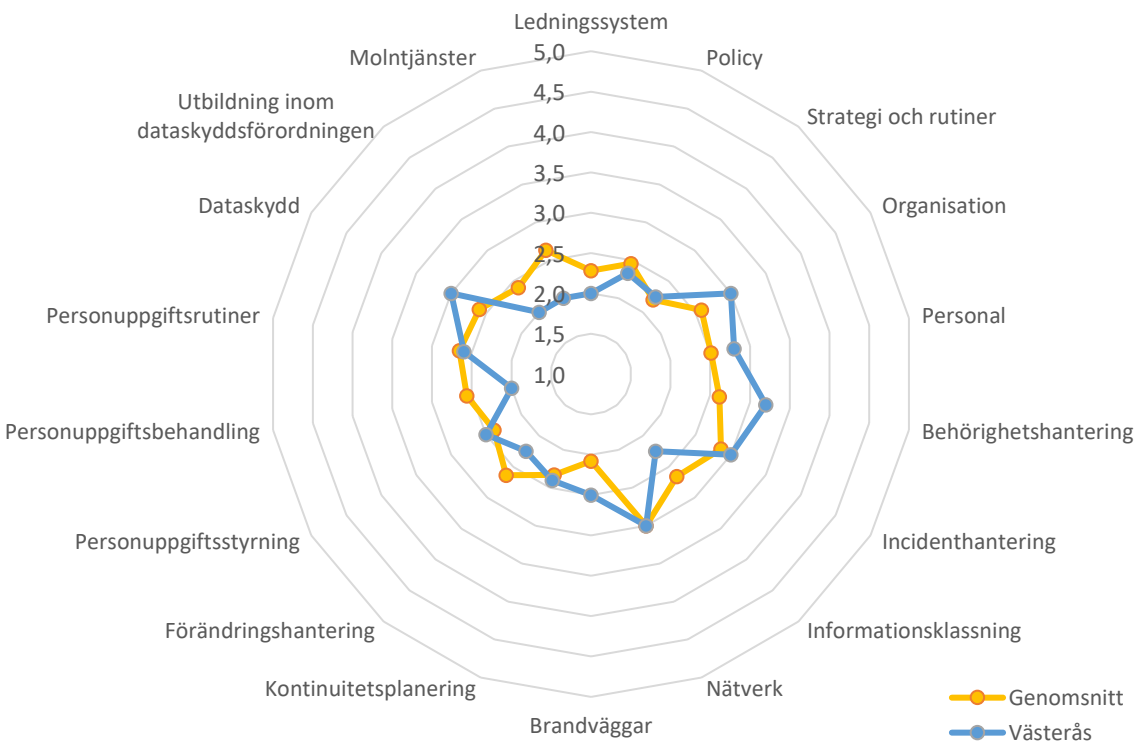
2 Analys

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stad är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

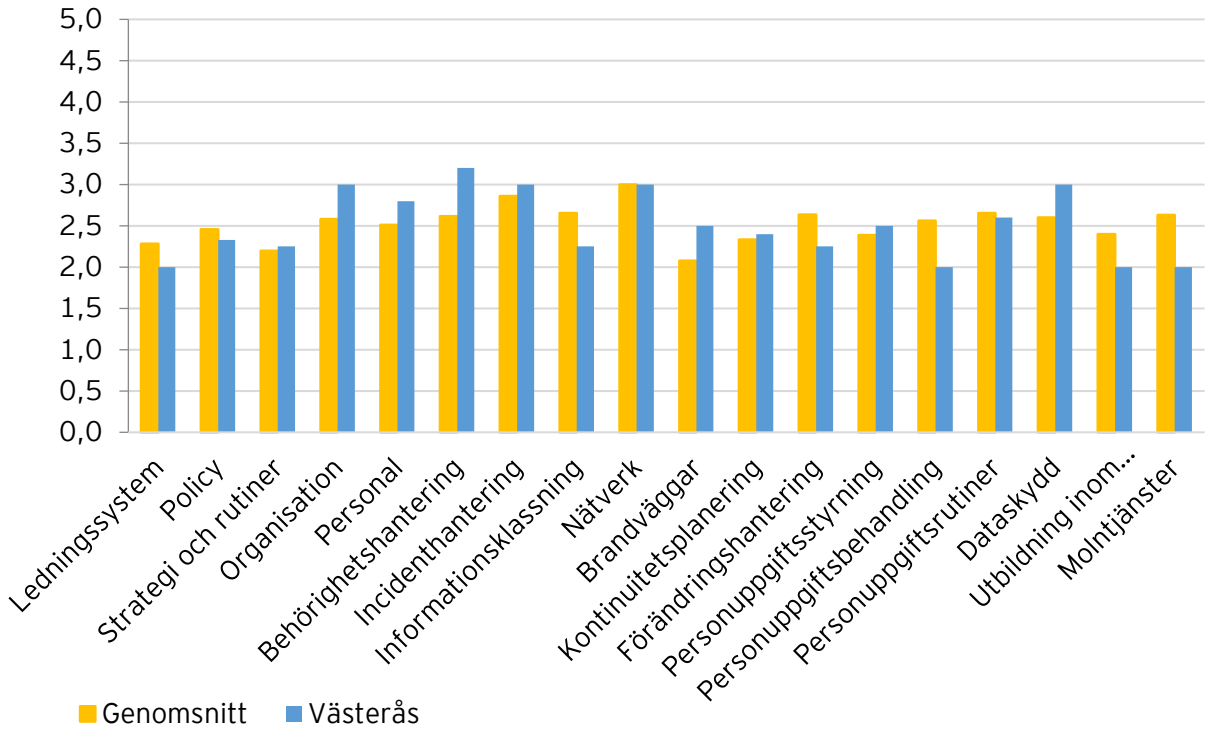
Västerås stad arbetar aktivt för att utveckla arbetet med informationssäkerhet. Bland annat bedrivs arbete för att uppdatera informationssäkerhetspolicyn. Mål om att expandera interna IT-säkerhetsutbildningar till medarbetare och nyanställa, samt att tydligare definiera dataskyddsombudens arbetsuppgifter utåt.

Kommunens främsta förbättringsbehov gäller upprättandet av en heltäckande internkontroll för IT- och informationssäkerhetsområdet. Behov för förbättring har även identifierats gällande kommunikation av policy och riktlinjer avseende IT- och informationssäkerhet, samt att upprätta en process för utbildning av informationssäkerhet för kommunens verksamhet.

Figur 1 nedan redovisar kommunens mognadsgrad för de 5 huvudområden som granskats samt en jämförelse med andra kommuner av motsvarande storlek och karaktär. Figur 2 visar detsamma fast nedbrutet på 18 underområden. Genomsnittet för andra offentliga organisationer av motsvarande storlek och karaktär är framtaget genom att bedöma mognadsgrad för samma områden och enligt samma metod som för Västerås stad.



Figur 1: Överblick över kommunens mognadsgrad för de 5 huvudområden som granskats i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.



Figur 2: Överblick över kommunens mognadsgrad för de 18 underområden i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.

2.1 Styrning

I sektionen nedan beskrivs nulägesbilden för huvudområdet *styrning* samt de iakttagelser som noterats under granskningens utförande (se Tabell 3).

Tabell 3: Nuläge och iakttagelser inom huvudområdet Styrning

Område	Nuläge	Iakttagelser	Mognad
Ledningssystem	Västerås stad har enligt styrande dokument inte etablerat ett Ledningssystem för informationssäkerhet (LIS) baserat på ISO/IEC 27001, Ledningssystem för informationssäkerhet. Kommunen har arbetat fram *riktlinjer för informationssäkerhet* baserat på ISO/IEC 27000 etablerat 2019 och arbetar med en *Handlingsplan för Ledningssystem för informationssäkerhet i Västerås stad* enligt given standard.	Kommunen har inte ett uppdaterat och helt fungerande Ledningssystem för informationssäkerhet (LIS).	2,00
Policy	Västerås stads arbete med informationssäkerhet beskrivs på en övergripande nivå i den nuvarande *informationssäkerhetspolicyn* upprättad 2011. I policyn fastställs Västerås stads syn på informationssäkerhet samt övergripande mål och roller. Informationssäkerhetspolicyn fungerar således som det överordnade och styrande dokumentet. Policyn beskriver kortfattat ansvarskrav avseende informationssäkerhet på olika roller inom kommunen, däribland *objektansvariga*, *stadsledningskontoret* och *informationsägarna*. Policyns övergripande mål är bland annat att leva upp till krav från användare av kommunens tjänster, förhålla sig till lagar och säkerställa godkända interna rutiner. Enligt policyn ska chefer på alla nivåer aktivt verka för kännedom hos medarbetare. Anställda hänvisas till policy och riktlinjer på intranätet. Vid upplärningsprocessen är det den nyanställdas ansvar att ta del av informationen i policy och riktlinjer. Att nyanställda ska ta del av policy och riktlinjer avseende IT- och informationssäkerhet finns dokumenterat i en särskild utbildningsprocess. Dock har processen ännu inte blivit implementerad då den vid tid för granskning planeras att lanseras inom kort. Vid tid för granskning bedrivs ett arbete inom kommunen att revidera *informationssäkerhetspolicyn*, med ett nuvarande utkast från 2022. Den reviderade policyn beslutas av kommunfullmäktige och utkastet innehåller i nuläget påbörjade tillägg såsom uppföljning.	Den gällande informationssäkerhetspolicyn är mer än 10 år gammal. Det saknas en dokumenterad process för hur det säkerställs att medarbetare kontinuerligt tar del av policy och riktlinjer avseende IT- och informationssäkerhet. En dokumenterad process för hur det säkerställs att nyanställda har tagit del av policy och riktlinjer avseende IT- och informationssäkerhet har ännu inte blivit implementerad.	2,33

Strategi och rutiner	Kommunens strategi avseende informationssäkerhet beskrivs i riktlinjerna. Riktlinjerna ska ses som ett minimumkrav för hantering av information, och de riktar sig till samtliga medarbetare inom kommunen. Det finns även dokumenterade riktlinjer för inköp och hantering av IT-relaterade produkter och tjänster inom kommunen. Riktlinjerna innefattar bland annat IT-säkerhet, styrning av IT samt målsättning med IT-arbetet. De nuvarande riktlinjerna avseende IT fastställdes under 2018 och är giltig tills 2021. Det saknas konkreta riktlinjer som beskriver vilka rutiner och säkerhetslösningar som behövs för att uppfylla de mål som beskrivs i informationssäkerhetspolicyn. Flertalet riktlinjer är äldre än 7 år.	Det saknas en definierad frekvens för hur ofta riktlinjer avseende informations-säkerhet ska granskas.	2,25
Organisation	Organisationen samt roll- och ansvarsfördelning för Västerås stad informationssäkerhetsarbete beskrivs i kommunens *informationssäkerhetspolicy* samt *riktlinjer för informationssäkerhet*. Informationssäkerhetspolicyn upprättas av kommunfullmäktige 2011. Det är denna policy som reglerar det övergripande arbetet med informationssäkerhet. I policyn beskrivs även de olika ansvarsområden inom detta arbete. I nuläget pågår även arbete om att uppdatera *informationssäkerhetspolicyn* och upprätta en mer detaljerad dokumentation över roller och ansvar inom informationssäkerhet hos kommunen. I den existerande policyn framgår det att årliga mål och ramar för informationssäkerhetsarbetet sätts upp i verksamhetsplaneringen. Ansvaret för informationen är decentraliserad och ligger hos respektive verksamhet. Det finns rådgivning tillgängligt i stadsledningskontoret i form av informationssäkerhetsstrateg. Varje dataskyddsombud agerar också som stöd till verksamheten. Det finns i nuläget inte några formaliserade kontroller eller rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet hos verksamheterna. Arbete på strategisk nivå inom informationssäkerhet ska ledas från stadsledningskontoret centralt. Informationssäkerhetsstrategen vid stadsledningskontoret har ansvaret för att samordna stadens arbete av informationssäkerhet. Beskrivning av informationssäkerhetsstrategens ansvar finns i *riktlinjer för informationssäkerhet*.	Styrdokumenten är till viss del utdaterade. Det saknas formaliserade kontroller och rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet hos verksamheterna.	3,00

	Informationssäkerhetsstrateg arbetar som stöd för verksamheten i informationssäkerhetsfrågor. Mer operativa arbeten ska skötas av objektägaren/objektledaren samt dataskyddssamordnare. Vid verksamhetsviktig information utses en eller fler informationsägare. Beskrivning av informationsägarens ansvar finns i *riktlinjer för informationssäkerhet*.		

2.2 Personal och behörigheter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personal och behörigheter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 4).

Tabell 4: Nuläge och iakttagelser inom huvudområdet Personal och behörigheter

Område	Nuläge	Iakttagelser	Mognad
Personal	Grundläggande informationssäkerhetsutbildning, kallat Nano-Learning, erbjuds för alla terminsvis – en på våren och en under hösten. De digitala utbildningarna är inte obligatoriska. För objektledare delas även information under nätverksträffar. Det finns en Nano-Learning för nyanställda, den är i nuläget inte obligatorisk men är planerad att bli det i framtiden. Vid nyanställning ansvar anställande chef för att den nyanställde tar del av utbildningen kring informationssäkerhet. Det är även varje användares ansvar att ta del av utbildningar och regelverk kring informationssäkerhet under anställningen. För objektägare sker nätverksträffar för utbyte av information och uppdateringar kring säkerhet. Samtliga av kommunens IT-system en utsedd systemägare. Kommunen har en dokumenterad rutin avseende säkerhet vid rekrytering för personal i vanlig såväl säkerhetsklassade befattningar. I *riktlinjen för informationssäkerhet* och *Instruktion Basnivå Informationssäkerhet* framgår det att säkerhetsprövningen ska innehålla kontroll av identitet. Säkerhetsprövning kan även inkludera bakgrundskontroll för medarbetare. Enligt riktlinjen ska det vid inhyrning av extern personal för utförande av tjänster åt staden upprättas sekretessavtal. Kommunens informationssäkerhetsfunktion är något underbemannad med resurser. Det dels på grund av nuvarande vakanta poster på stadsledningskontoret.	Utbildning i informationssäkerhet är inte obligatoriskt. Det saknas obligatorisk utbildning i informationssäkerhet till nyanställda.	2,80
Behörighets-hantering	Kommunen har en definierad process för behörighetshantering som är beskriven i kommunens		3,20

	basnivå informationssäkerhet och *riktlinje för informationssäkerhet*. Dokumenten är fastställda 2015 respektive 2019. Höga behörigheter ska inte tilldelas fler individer än nödvändigt, och samtliga höga behörigheter ska vara individuella behörigheter. Behörigheter med åtkomst till infrastruktur förekommer inte eftersom kommunen inte äger någon infrastruktur då detta hanteras av extern driftleverantör. Kommunen har i avtal ställt krav på leverantören att endast säkerhetsprövad personal får ha tillgång till infrastrukturen. Instruktioner för behörighetskontroll finns i *Instruktion åtkomst till system och nätverk*. Däri finns även styrning av systemadministrativa behörigheter. Dokumentet är fastställt 2015. Genomgång av användarbehörigheter ska genomföras minst årligen, och det är objektledarens ansvar att göra detta. Genomgången ska inkludera en verifiering av att personerna i fråga har ett oförändrat åtkomstbehov. Behörigheter ska tas bort vid avslutad tjänst. Genomgång av behörigheter hanteras i samband med klassning av system, det finns i handlingsplanen en uppföljningsplan om att ta fram den typen av rutiner i objektsledningen. I de allra flesta system så skickas beställningar på roller/systembehörigheter i ett beställningsflöde till ansvarig chef, enligt anvisning på Insidan. Vid tid för granskning finns det ingen dokumenterad process för att säkerställa en lämplig segregering av roller och behörigheter inom både organisationen och informationssystemen. Kommunen har en lösenordspolicy. Det finns tre nivåer av lösenordsregler baserat på karaktären av kontot med ökande krav av svårighetsgrad. Enligt de intervjuade nyckelpersonerna lever dessa lösenordsinställningar upp till kraven i lösenordspolicyn för samtliga system. Det är tjänsteansvarig för IT-infrastrukturen som ansvarar för lösenordspolicyn och hanteringen av den.	Det saknas en dokumenterad process avseende att systemägare ska dokumentera genomförandet av periodisk genomgång av behörigheter. Kommunen saknar en dokumenterad process för att säkerställa segregering av roller och behörigheter inom organisation och system. Det finns ingen dokumenterad uppföljning på att lösenordspolicyn följs.	

2.3 Drift

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *drift* samt de iakttagelser som noterats under granskningens utförande (se Tabell 5).

Tabell 5: Nuläge och iakttagelser inom huvudområdet Drift

Område	Nuläge	Iakttagelser	Mognad

Incident-hantering	Enligt *riktlinjer för informationssäkerhet* ska säkerhetsincidenter som misstänks kunna påverka informationssäkerheten rapporteras till närmsta chef utan dröjsmål. Gäller det fel och/eller brister i systemet ska dessa även rapporteras till objektägaren. IT- och informationssäkerhetsincidenter rapporteras genom att fylla i en standardiserad mall. Hanteringen av säkerhetsincidenter beskrivs i *Instruktion för säkerhetsincidenthantering*. Dokumentet beskriver ansvar och roller mellan staden och IT-leverantören, principer för prioritering, med mera. Instruktionen saknar dock en beskrivning för hur säkerhetsincidenter ska följas upp på aggregerad nivå, vilket kan försvåra för staden att kontinuerligt förbättra såväl processen, som den faktiska hanteringen. Enligt intervjuade personer följs incidenter upp i *säkerhetsforum* tillsammans med leverantören. Säkerhetsincidenter loggas alltid. Mindre ärenden, som inte ses som incidenter, loggas som ärenden.	Incidenthanteringsprocessen beskriver inte hur uppföljning av incidenter på aggregerad nivå ska ske.	3,00
Informations-klassning	Västerås stad använder en modell för klassificering som bygger på Myndigheten för Samhällsskydd och beredskaps (MSB) och SKL:s rekommendationer som i sin tur utgår ifrån ISO/IEC 27000-standard för informationssäkerhet. Västerås informationshantering styrs till stor del av bestämmelser i Tryckfrihetsförordning (1949:105) och Offentlighets- och sekretesslag (OSL) 2009:400. Vidare hanteras en stor del information som lyder under Personuppgiftslagen (PuL) 1998:204.	Västerås stad hänvisar fortfarande till stor del till PuL.	2,25
Nätverk	Kommunen har ett dokument som beskriver nätverksdesign. Dokumentet innefattar bland annat nätverkssäkerhet, brandväggsadministration och nätverkssegmentering. Det beskrivs även hur nätverkstrafik ska styras. Dokumentet är upprättat av IT-direktör 2014. Kommunen har implementerat Intrusion Prevention System (IPS) och Intrusion Detection System (IDS) för att analysera nätverksaktivitet.	Nätverksdokumentationen är gammal och bör revideras.	3,00
Brandväggar	Västerås stad har ett brandväggsråd som ska sammanträda varje vecka. Brandväggsrådet hanterar externa och interna brandväggar och brandväggsregler på servrar och klienter. Det finns upprättade rutiner och instruktioner för hur ändringar i brandväggar ska göras och varje ändring granskas och godkänns innan förändringen genomförs. Ingen dokumenterad brandväggspolicy för att styra underhåll och dokumentation av brandväggsrelaterade aktiviteter finns.	Det finns ingen upprättad brandväggspolicy, -instruktion eller liknande.	2,50

	Enligt rutin för ansökan om portöppning ska ansökan beställas av objektledare och följa en förutbestämd mall med information. En godkänd portöppningsansökan signeras av ordförande för brandväggsrådet. Ingen dokumenterad granskning av brandväggsskyddet finns.	Brandväggarnas funktion och konfiguration granskas inte.	
Kontinuitetsplanering	Kontinuitetsplanering beskrivs övergripande i *riktlinje för informationssäkerhet* och inkluderar vad en kontinuitetsplan i verksamheten ska omfatta. Verksamhetsansvarig chef ansvarar för att det finns en kontinuitetsplan dokumenterad. Det kan förekomma små, eller nyligen produktionssatta, system utan kontinuitetsplan. Det finns en kundkontinuitetsplan där det finns definierat vad en katastrof och kris innebär för Västerås stad. Den är en bilaga i avtal, och det regleras där. Det finns rutiner för att testa stadens känsligare system i driftpartnerns årshjul, där bl.a. återläsningstest genomförs. Kontinuitetsplanerna följs inte upp och testas inte på regelbunden basis.	Det saknas en rutin för att följa upp och testa kontinuitetsplaner.	2,40

2.4 Programförändringar

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *programförändringar* samt de iakttagelser som noterats under granskningens utförande (se Tabell 6).

Tabell 6: Nuläge och iakttagelser inom huvudområdet Programförändringar

Område	Nuläge	Iakttagelser	Mognad
Förändrings-hantering	Rutiner för förändringshantering ska finnas etablerade inom systemets förvaltningsorganisation, och vara framtagen i samråd med IT-driftleverantör. Respektive systemägare ansvarar för att hålla systemet uppdaterat. Därtill ligger ansvaret hos systemförvaltaren att det ska finnas en förvaltningsplan för systemet. Enligt instruktion ska alla ändringar av programvara vara formellt godkända innan den installeras i utbildnings-, acceptanstest- eller produktionsmiljö. Det ska även finnas ett testprotokoll som är undertecknat av styrgrupp eller motsvarande. Alla program har inte testmiljöer. Samtliga ändringar ska vara spårbara och de ska kunna härledas till en ansvarig beställare. Övervakningsrutiner för driftmiljöer som säkerställer att inga programförändringar införs som inte är godkända ska vara implementerade.	För vissa system testas förändringar direkt i produktionsmiljön.	2,25

	Ändringar i driftmiljön i system som utbyter information med andra system (integrationer) ska följa stadens riktlinjer för systemintegration. Avtalet mellan kommunen och den externa driftleverantören ska beskriva en tydlig process för förändringshantering som inkluderar att samtliga förändringar protokollförs. En 'Patch Tuesday' äger rum en gång i månaden för att få in mindre uppdateringar enligt ett regelbundet schema.		

2.5 Personuppgifter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personuppgifter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 7).

Tabell 7: Nuläge och iakttagelser inom huvudområdet Personuppgifter

Område	Nuläge	Iakttagelser	Mognad
Personuppgifts-styrning	Västerås stads riktlinjer innefattar bland annat att personuppgifter endast får samlas in för berättigade ändamål samt att personuppgifter inte får sparas längre än nödvändigt. Det finns ett dokument för konsekvensbedömning (DIPA), för personuppgiftsbehandling. Det finns en dokumenterad process för registerutdrag där det framgår hur kommunen ska hantera en begäran. Granskning av dataskyddsarbetet sker framför allt på verksamhetsnivå där de besvarar ett antal kontrollfrågor utformat av dataskyddsorganisationen som sedan DSO sammanställer, analyserar och använder för att ge råd för det fortsatta arbetet med GDPR. Dataskyddsombuden sätter ihop en granskningsrapport som återrapporteras till nämnderna. Ingen efterlevnadsutvärdering görs på förvaltningarna. I riktlinje för dataskyddsarbetet finns mycket information för verksamheterna kring dataskyddsombuden, mindre information kring arbetet som utförs. En ny version håller på att tas fram, med ett delsyfte att förbättra detta.	Västerås stad har ett flertal dokument upprättade före 2018 som refererar till PuL i samband med personuppgifter. Kommunen har ej säkerställt att styrande dokument avseende GDPR förblir riktiga och aktuella över tid. Uppföljning förlitar till stor del på självutvärdering i verksamheterna. Riktlinje för dataskyddsarbete fokuserar lite på hur personuppgifter faktiskt ska hanteras.	2,50

Personuppgifts-behandling	Kommunstyrelsen och varje nämnd har eget ansvar för att de personuppgifter som behandlas i deras verksamhet sker lagligt och korrekt enligt centrala riktlinjer. Kommunens registerförteckning innefattar cirka 65 personuppgiftsbehandlingar. Vissa ändamål i kommunstyrelsens registerförteckning saknar uttalad rättslig grund. Det saknas även fullständiga registerförteckningar hos vissa nämnder. Kommunen upprättar PuB-avtal med leverantörer som hanterar kommunens personuppgifter enligt SKR-avtalsmall. Avtalen innefattar bl.a. ansvar, säkerhetsåtgärder och sekretess.	Registerförteckningen är inte fullständig och korrekt för alla delar i Västerås stad.	2,00
Personuppgifts-rutiner	Kommunen har dokumenterade instruktioner för personuppgiftsincidenter. Medarbetare ska vid osäkerhet kontakta och samråda med dataskyssombud på stadsledningskontoret. Personuppgiftsincidenter loggförs för att hålla koll på antalet incidenter som uppstår. Dataskyddssamordnare inom verksamheterna ansvarar för samordning och agerar kontaktperson mot dataskyddsombuden på stadsledningskontoret. Gallringsplaner ligger hos respektive verksamhet. Västerås stad har ett fastställt dokument för hantering av skyddade personuppgifter.	Krav på gallring saknas centralt.	2,60
Dataskydd	För att etablera ett allmänt dataskydd inom kommunen har åtgärder vidtagits i form av riktlinjer för IT-stöd. I *Instruktion Basnivå IT-säkerhet* finns specifika instruktioner gällande planering och godkännande av IT-stöd, åtgärder mot skadlig kod och säkerhetsuppdateringar. Instruktionen är fastställd 2015. Kommunstyrelsen och varje nämnd besitter eget ansvar över de personuppgifter de hanterar. Dataskyddsombuden hjälper till med stöd till verksamheterna samt leder och samordnar dataskyddarbetet i Västerås stad.	Instruktioner för IT-säkerhet revideras ej med fastställda intervaller. Genom att både implementera och granska dataskydd riskerar DSO att granska sitt eget arbete.	3,00
Utbildning inom dataskydds-förordningen	GDPR-utbildningar utförs genom Nano-Learning, vilket innebär regelbundna korta internetutbildningar. Utbildning ges till samtliga medarbetare terminsvis. Utbildningarna följs ej upp med avseende på deltagande. Det är verksamhetschefernas ansvar att se till att samtliga anställda inom verksamheten har genomfört utbildningarna.	Västerås stad följer inte upp vilka medarbetare som deltar i Nano-Learnings.	2,00

	Underlag finns från dataskyddsutbildning på stadsledningskontoret där ansvar och krav gås igenom. Dessa utbildningar ansvaras för, och leds av dataskyddsombudet.		
Molntjänster	Kommunen hanterar personuppgifter i molntjänster. En särskild säkerhetsanalys ska göras för anslutningar via molntjänster. Enligt *Instruktion anskaffning av IT stöd* ska anskaffning av molntjänster följa samma procedur som vid outsourcing till extern leverantör. Det finns ett kravbibliotek för staden där krav kan väljas i de fall som ett införande ska ligga i molnet. Dokumentationen hänvisar till lathund av Myndigheten för Samhällsberedskap (MSB) för stöd vid anskaffning. Tekniska krav på molntjänstleverantörer framgår inte.	Västerås stad har ingen sammanställd riktlinje specifikt för molntjänster Det finns ingen teknisk kravspecifikation på molntjänster.	2,00

3 Övergripande rekommendationer

Granskningen har identifierat iakttagelser inom flera delar av ramverket. EY har valt att presentera de mest relevanta rekommendationerna för Västerås stad och förslag på åtgärder för de främsta riskerna inom IT- och informationssäkerhetsarbetet.

Revision av styrdokument och riktlinjer

Riktlinjer och styrdokument avseende informationssäkerhet saknar vid tid för granskning en definierad frekvens för hur ofta de ska revideras. Kommunstyrelsen rekommenderas tillse att riktlinjer avseende IT- och informationssäkerhet revideras kontinuerligt utefter ett förutbestämt tidsintervall för att säkerställa att riktlinjer förbli riktiga och aktuella över tid. Kommunstyrelsen rekommenderas även tillse att granskning av riktlinjer dokumenteras även i de fall ingen förändring av dokumenten utförs.

Kommunikationsplan

Kommunikation av policy och riktlinjer sker i praktiken enligt flertalet metoder som inte är dokumenterade. Kommunstyrelsen rekommenderas tillse att en dokumenterad kommunikationsplan för policy och riktlinjer avseende IT- och informationssäkerhet upprättas. Kommunikationsplanen bör indikera vem som ansvarar för att kommunicera policy och riktlinjer till medarbetare inom kommunen samt på vilket sätt detta ska göras.

Utbildningsplan

Utbildning för informationssäkerhet på generell nivå saknar dokumenterad utbildningsplan och systematisk uppföljning av utbildningarnas genomförande. Kommunstyrelsen rekommenderas att ta fram en dokumenterad utbildningsplan för såväl långvariga medarbetare som nyanställda och säkerställa att genomförandet av utbildningar bland medarbetare kontinuerligt följs upp. Dessutom rekommenderas en undersökning av kunskapsbehoven hos medarbetare och därefter anpassade utbildningsinsatser.

Internkontrollplan, samt uppföljning och efterlevnad

Dataskyddsombud sammanställer vartannat år självutvärderingar hos förvaltningar gällande dataskyddsförordningen. Det saknas dock formaliserade kontroller och rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet som helhet i Västerås stads nämnder och förvaltningar. Kommunstyrelsen rekommenderas tillse att en internkontrollplan avseende IT- och informationssäkerhet upprättas som är heltäckande för de olika områdena inom kommunens IT- och informationssäkerhetsarbete. Genom en heltäckande internkontrollplan kan kommunstyrelsen kontrollera efterlevnad av policy och riktlinjer avseende IT- och informationssäkerhet samt upptäcka eventuella gap.

4 Revisionsfrågor

Granskningen har utgått från revisionsfrågan: bedriver Västerås stad ett tillräckligt och ändamålsenligt IT- och informationssäkerhetsarbete? Revisionsfrågan har brutits ner och besvarats enligt nedan.

Tabell 8: Förklaring av färgkod

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvaras delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Tabell 9: Svar på revisionsfrågor

Revisionsfråga	Svar	
▸ **Kan *styrningen* av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamheter har, bedömas som ändamålsenligt?**	Styrningen av kommunens arbete med IT- och informationssäkerhet bedöms vara delvis ändamålsenlig. Svaret grundar sig i att kommunen har flertalet upprättade styrdokument för att styra och organisera IT- och informationssäkerhetsarbetet. Det finns en informationssäkerhetspolicy samt riktlinjer som beskriver flera områden inom IT- och informationssäkerhet. Dock saknas det en definierad frekvens för hur ofta riktlinjer ska uppdateras - vilket kan leda till att riktlinjer inte förbli riktiga och aktuella över tid. Vidare saknas en dokumenterad process för att kontinuerligt säkerställa att anställda har tagit del av och har kännedom om policy och riktlinjer avseende IT- och informationssäkerhet. Kommunen har dokumenterade riktlinjer avseende personuppgiftshantering. Riktlinjer avseende hantering av personuppgifter och registrerades rättigheter enligt GDPR har däremot inte blivit uppdaterade sedan 2019. En del dokumentation refererar till PuL som upphörde att gälla 2018. Vidare saknas lokalt anpassade riktlinjer avseende GDPR för nämnder/verksamheter inom kommunen.	

▸ **Är arbetet med att *följa upp* att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?**	Uppföljningen av efterlevnad av kommunens arbete med IT- och informationssäkerhet bedöms vara delvis ändamålsenlig. Svaret grundar sig i att det genomförs riskanalys årligen av system som hanterar personuppgifter eller verksamhetsinformation. Det genomförs även en årsvis utvärdering av GDPR-arbetet för att kontrollera hur kommunen efterlever GDPR. Uppföljningsarbetet bedöms inte vara fullständigt ändamålsenligt då det saknas en dokumenterad process för att säkerställa att det sker kontroll eller uppföljning av samtliga områden inom kommunens IT- och informationssäkerhetsarbete samt att deltagande på utbildningar inom informationssäkerhet inte följs upp.	
▸ **Är Västerås stads *incidenthanteringsprocess* ändamålsenlig?**	Kommunens incidenthanteringsprocess bedöms vara delvis ändamålsenlig. Svaret grundar sig i att kommunen har en dokumenterad process för IT- och informationssäkerhetsincidenter, samt ett formulär för att anmäla dessa incidenter. Kommunen har även en separat process samt formulär för anmälan av personuppgiftsincidenter. Incidenthanteringsprocessen beskriver dock inte hur staden systematiskt ska följa upp incidenter för att kunna förbättra såväl incidenthanteringen sig samt själva processen.	
▸ **Har tillräckliga åtgärder vidtagits av staden med anledning av de rekommendationer som revisionen lämnade vid sin granskning av stadens arbete med GDPR?**	Åtgärderna av stadens arbete med GDPR bedöms vara delvis ändamålsenlig. Svaret grundar sig i att kommunen har tillfört viss dokumentation för hantering av personuppgifter utifrån GDPR. Dock så finns gamla dokument utan hänvisning till GDPR som inte har reviderats sedan innan dataskyddsförordningen trädde i kraft 2018.	

5 Slutsatser

Granskningens syfte har varit att bedöma om det finns brister i kommunens interna kontroll avseende informationssäkerheten. Vidare har syftet också varit att bedöma i vilken omfattning kommunstyrelse och nämnder styr och följer upp detta arbete.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stad är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad.

EY:s övergripande bedömning är att Västerås stad arbete med IT- och informationssäkerhet är delvis ändamålsenligt. Bedömningen grundar sig i att kommunen har en väldefinierad organisation och ändamålsenliga styrdokument avseende IT- och informationssäkerhet på plats. Däremot saknas vissa formaliserade processer avseende kontinuerlig kommunikation och revision av styrande dokument. Bedömningen grundar sig även i att det saknas en formaliserad process för att säkerställa att samtliga medarbetare genomför relevant utbildning inom informationssäkerhet.

Med grund i ovan är EY:s främsta rekommendationer att kommunstyrelsen i Västerås stad tillser att:

- En plan upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Stockholm 2022-12-13

Helena Törnqvist, Partner

Bilaga 1: Källförteckning

Intervjuade roller:

- Verksamhetschef
- Tillförordnad projektledare inom digitalisering
- Informationssäkerhetsstrateg
- Säkerhetschef
- Dataskyddsombud

Dokumentförteckning:

- 150129_Instruktion logghantering och spårbarhet v 1_0
- 150319_Instruktion Basnivå Informationssäkerhet v 1_0
- 150417_Instruktion Anskaffning utv och under av is v 1_0
- 150417_Instruktion Åtkomst till system och nätverk v 1_0
- 150518 Instruktion Basnivå IT-säkerhet v 1_0
- 160309 Instruktion Skyddade personuppgifter v 1_0 Dnr 2016_169_KS_009
- Begäran om registerutdrag - ifyllnadsbar PDF
- Bilaga 1, bekräftelsebrev registerutdrag (1)
- Bilaga 1, Checklista vid utredning av personuppgiftsincident
- Bilaga 2, Rapport - Dataskyddsombudets omedelbar bedömning
- Bilaga 2, registerutdrag
- Bilaga 3, Ordförandebeslut - Beslut om anmälan till integritetsskyddsmyndigheten
- Bilaga 4, Beskrivning av personuppgiftsincident
- Dataskydd - Västerås stad Intranät
- Digitaliseringsenhetens styrande dokument
- DPIA - Konsekvensbedömning - mall (1)
- Handlingsplan for digital fornyelse-2019
- Handlingsplan Ledningssystem för informationssäkerhet_2022
- Instruktion anskaffning av IT-stöd
- Instruktion för arbete med registerutdrag
- Instruktion för hantering utav personuppgifter i Västerås stad
- Instruktion för radering och rättelse (1)
- Kompletterande instruktion till PUB, version 3
- Lösenordsbyten - Västerås stad Intranät
- Målbild i avtalet om Säkerhetstjänster
- PUB-avtal, KS eller enskild nämnd som PUA, leverantör som PUB, version 2.0, slutversion mall
- Rapportmall
- Registerförteckning KS
- Riktlinje för dataskyddsarbetet i Västerås stad, version 2, 2020-09-08
- Riktlinje_för_digitala_verktyg_och_telefonitjänster_V2_fastställd
- Riktlinje för informationssäkerhet
- Riktlinje för utskriftstjänster 2021
- Riktlinjer för nätverksdesign
- Riktlinjer för systemintegration
- Rutin för ansökan om portöppning för Västerås stad till TietoEVRY 2022
- Rutiner för konsekvensbedömning (1)
- Roller i Västerås stads organisation för informationssäkerhet_utkast_220315
- Roller i Västerås stads organisation för informationssäkerhet_utkast_220325
- Samverkansavtal mellan leverantörer

- Stadsgemensam informationshanteringsplan version 2020 1.2
- Styrning och samverkan
- Styrning och samverkan 1.0
- Säkerhetskrav
- Tjänsteavtal - IT drift
- Tjänstebilaga Säkerhetstjänster
- Utbildning SK
- Utskick sökning registerutdrag
- Vägledning grundläggande kryptering för kommentarer
- Vägledning för fysisk säkerhet i IT-utrymmen

Bilaga 2: Definitioner

Change Advisory Board: En konstellation av IT- och verksamhetsrepresentanter som stödjer processen avseende förändringar genom att ge råd och fatta beslut.

Dataskyddsombud (DSO): Särskilt utsedd person vilken tillser att personuppgifter behandlas på korrekt och lagenligt sätt inom organisationen, genom att till exempel utföra kontroller och utbildningsinsatser.

Data Protection Impact Assessment (DIPA): En konsekvensbedömning som beskriver syftet med personuppgiftsbehandlingen och de risker som kan uppstå för personen vars uppgifter behandlas.

Informationsklassning: Klassning av informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet, tillgänglighet och konfidentialitet.

Informationssäkerhet: Säkerhetsfrågor som berör information, oberoende av system och plattformar.

Informationssäkerhetssamordnare: Särskilt utsedd person som innehar det övergripande ansvaret att leda och samordna utvecklingen av kommunens informationssäkerhet.

Intrusion detection system (IDS): Ett verktyg som används för att upptäcka intrång eller intrångsförsök i ett datasystem.

Intrusion prevension system (IPS): Ett verktyg som används för att upptäcka och reagera intrång eller intrångsförsök i ett datasystem.

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurering.

ITIL V3: ITIL (Information Technology Infrastructure Library) är ett ramverk för att standardisera IT-relaterade aktiviteter. ITIL V3 är en version som även inkluderar strategiska element i syfte att IT bättre ska sammanvävas med verksamheten.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

Ledningssystem: Definierat verktyg eller system för att leda, planera, kontrollera, följa upp och utvärdera den egna verksamhetens arbete med informationssäkerhet.

Molntjänster: Tjänster och system som inte drivs lokalt av kommunen och som nås via en internetuppkoppling och inte direkt via det lokala nätverket.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.

Patchning: Tillägg till ett program eller system avsett att rätta till sårbarheter.

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.

Objektägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.