Granskning av informationssäkerhet i skolsystemet IST Administration

Rapport

Göteborgs stad

KPMG AB

Datum 2023-01-11

Antal sidor 28

Göteborgs Stad
Granskning av informationssäkerhet i IST Administration

2023-01-11

Innehållsförteckning

1 Sammanfattning

KPMG har av stadsrevisionen i Göteborg fått i uppdrag att granska grundskolenämndens och utbildningsnämndens informationssäkerhetsarbete avseende det skoladministrativa systemstödet IST-administration. Uppdraget ingår i revisionsplanen för år 2022.

Vår sammanfattande bedömning utifrån granskningens syfte är att grundskolenämnden och utbildningsnämnden endast delvis bedriver ett informationssäkerhetsarbete som säkerställer konfidentialitet, riktighet och tillgänglighet i de informationstillgångar som hanteras i det skoladministrativa systemstödet IST-administration.

Granskningen visar att nämnderna inte fullt ut etablerat ett systematiskt informationssäkerhetsarbete i enlighet med interna styrdokument och har därigenom brustit i sitt ansvar som informationsägare. Bland annat har inte väsentliga aktiviteter för att analysera och bedöma risker för den information som hanteras i IST Administration genomförts av nämnderna. Utan detta saknas underlag för att besluta om säkerhetsåtgärder som står i relation till hur skyddsvärd den information som hanteras i systemet är för respektive nämnd.

Vid tiden för granskningen saknades för båda nämnderna etablerade förvaltningsorganisationer för IST Administration. Detta riskerar att försvåra uppföljningsarbetet i förhållande till de informationssäkerhetskrav som ställts på leverantören. Efterlevnad utifrån avtalade nivåer har inte kontrollerats sedan 2019 då detta genomfördes av den dåvarande projektorganisationen inom nämnden för Intraservice. De krav på en regelbunden analys av risker som behövs för att säkerställa tillräckliga skyddsåtgärder, som riktlinje för informationssäkerhet reglerar, har därigenom inte efterlevts av nämnderna. Det har inte skett någon årlig uppföljning och rapportering till nämnderna om informationssäkerhetsnivån för systemet. Det är väsentligt att nämnderna är uppdaterade om aktuella hot och risker avseende informationssäkerhet så att beslut om åtgärder kan fattas.

2 Bakgrund

KPMG har av stadsrevisionen i Göteborg uppdragits att genomföra en granskning av grundskolenämndens och utbildningsnämndens informationssäkerhetsarbete avseende det skoladministrativa systemstödet IST-administration.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används för information som hanteras i stadens IT-system. Alltmer information hanteras idag med olika tekniska lösningar och aldrig förr har sådana mängder information hanterats som idag. Informationssäkerhet innebär att skydda information utifrån krav på konfidentialitet, riktighet och tillgänglighet. För att kunna hantera detta på ett ändamålsenligt sätt krävs att staden har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget. Informationssäkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av stadens kärnverksamheter.

Skolverksamheter kännetecknas av en hög koncentration av information. En förutsättning för att rätts- och informationssäkert hantera dessa informationsmängder är att verksamheterna har tillgång till väl fungerande IT-system.

I sin revisionsplan för år 2022 konstaterar revisorerna att staden hanterar stora mängder skyddsvärd information och att detta flöde ofta hanteras med hjälp av olika IT-system och integrationer dem emellan. Då hanteringen av informationsmängder utgör en förutsättning för att stadens verksamheter ska kunna utföra sina uppdrag blir frågan om informationssäkerhet av särskild betydelse. Brister i informationssäkerhet kan få allvarliga konsekvenser, till exempel att integritetskänslig information får spridning eller att verksamhetskritiska processer stannar. Revisorerna identifierar som en följd av denna analys IT-system och informationssäkerhet som ett särskilt riskområde och en prioriterad inriktning för granskning under åren 2022 till 2024.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om nämnderna bedriver ett informationssäkerhetsarbete som säkerställer konfidentialitet, riktighet och tillgänglighet i de informationstillgångar som hanteras i det skoladministrativa systemstödet IST-administration.

Granskningen har besvarat följande revisionsfrågor:

- Har nämnderna säkerställt att det för IST-administration finns en ändamålsenlig organisation med en tydlig roll-, ansvars-, och befogenhetsfördelning i informationssäkerhetsarbetet?
- Har nämnderna säkerställt att det finns rutiner som medför att lämnade behörigheter att ta del av, ändra eller lägga till information i IST- administration är aktuella och korrekta?
- Har nämnderna säkerställt att skyddade personuppgifter hanteras på ett sådant sätt att de inte röjs för obehöriga?
- Har nämnderna säkerställt att säkerhetsmonitorering inkluderande loggning av säkerhetsrelevanta händelser sker på ett ändamålsenligt sätt i IST-administration?
- Har nämnderna säkerställt att det för IST-administration finns tillfredsställande rutiner för backup av program och data, samt för återläsning av data?
- Har nämnderna säkerställt att det för IST-administration finns en aktuell, dokumenterad och beslutad kontinuitetsplan?
- Har nämnderna säkerställt att informationssäkerhetsnivån i IST- administration löpande är acceptabel, att den följs upp årligen och att nämnden erhåller en rapport av resultaten av denna uppföljning?

Granskningen avser Göteborgs Stads grundskolenämnd samt utbildningsnämnd.

2.2 Revisionskriterier

Följande revisionskriterier har använts i granskningen:

- Kommunallagen 6 kap § 6
- Offentlighets- och sekretesslagen, 21 kap 3 §
- Göteborgs Stads riktlinje för informationssäkerhet
- Göteborgs Stads regel gällande driftsdokumentation för IT-baserade informationssystem
- Göteborgs Stads regel för IT-användare
- Göteborgs Stads regel för chefers informationssäkerhetsansvar

2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med tjänstepersoner inom utbildningsförvaltningen, grundskoleförvaltningen samt representanter från NAIS[1]-projektet.

Dokumentstudier har omfattat:

- Systemdokumentation och informationssäkerhetskrav
- Informationsklassning
- Teknisk riskanalys

[1] Projektet för implementering av nytt administrativt IT-stöd för utbildningsverksamheten heter NAIS. Projektet bedrevs fram till och med 2022-07-31 i Intraservice regi, för att sedan dess bedrivas med de tre skolförvaltningarna som gemensam huvudman, med administrativ placering på utbildningsförvaltningen.

- Rapport för efterlevnadskontroll
- Konsekvensbedömningar
- Riktlinje och rutiner för hantering av elever med skyddade uppgifter
- Rutin och instruktioner för behörighetshantering

Rapporten är faktakontrollerad av samtliga intervjupersoner.

3 Resultat av granskningen

3.1 Organisation och ansvar

3.1.1 Ansvar för informationssäkerhet

I Göteborgs Stads säkerhetspolicy[2], vilken är överordnad Riktlinje för informationssäkerhet[3], regleras ansvaret för säkerhetsfrågorna. Av policyn framgår att nämnderna är ansvariga för säkerheten inom respektive verksamhet. Förvaltningsledningen ska genom tydlig inriktning och fördelning av ansvar engagera sig i verksamhetens säkerhetsarbete samt minst årligen följa upp att säkerhetsnivån är acceptabel med återrapportering till nämnd.

Enligt riktlinjen för informationssäkerhet är informationsägare ”den som bestämmer ändamålen med och medlen för behandling och hantering av informationen. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten”.

Det finns enligt intervjuade vissa oklarheter avseende vem som ska bära informationsägarskapet i förvaltningarna. Det mest troliga anges vara att förvaltningscheferna ska vara informationsägare.

Både utbildningsförvaltningen och grundskoleförvaltningen har utsedda informationssäkerhetssamordnare i respektive verksamhet. Enligt intervjuade inom grundskoleförvaltningen och utbildningsförvaltningen saknas en tydlighet över vilka uppgifter som åligger informationssäkerhetssamordnaren. Inom utbildningsförvaltningen har ytterligare en informationssäkerhetssamordnare anställts som ska ha ett mer operativt ansvar för IT-säkerhetsfrågorna. När den nya

[2] Beslutad av kommunfullmäktige, reviderad senast 2019-12-16. Dnr 0540/14 (0110/19).

[3] Beslutad av kommunfullmäktige, reviderad senast 2019-12-16. Dnr 0540/14 (0110/19).

samordnaren är på plats ska enligt intervjuade en tydligare fördelning av uppgifter göras.

Enligt riktlinjen för informationssäkerhet ska informationsklassning göras kontinuerligt av informationsägaren och ligga till grund för hur informationen ska hanteras i verksamheten. I ansvaret ingår att erforderliga skyddsåtgärder införs samt att säkerheten uppfyller ställda och rättsliga krav.

Vi har i granskningen tagit del av en informationsklassning från 2020 där informationsklassningsbeslutet är undertecknat av avdelningschefen för digitalisering och innovation inom Intraservice. Informationsklassningen har resulterat i bedömningen att säkerheten som minimum ska uppfylla Göteborgs Stads grundsäkerhetsnivå avseende tillgänglighet samt förhöjd säkerhet avseende konfidentialitet och riktighet.

Vi har i granskningen tagit del av båda nämndernas konsekvensbedömningar för de personuppgiftsbehandlingar som sker i IST Administration. Konsekvensbedömningarna är uppdaterade och aktuella[4]. Att göra konsekvensbedömningar är ett krav enligt dataskyddsförordningen, för de personuppgiftsbehandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (art 35.1)”.

Som förklaring till att inte utbildningsförvaltningen har någon aktuell riskanalys eller uppdaterad informationsklassning för IST Administration anges att de gjort bedömningen att informationssäkerhetsrisker och dataskyddsrisker överlappat varandra. Intervjuad från utbildningsförvaltningen anger att det främst varit personuppgifterna som utgjort de mest väsentliga riskerna.

[4] Grundskolenämnden 2022-09-15 och Utbildningsnämnden 2022-06-21

3.1.2 Ansvar för IST Administration

Riktlinje för informationssäkerhet anger att säkerhetsaspekter ska beaktas vid anskaffning av informationssystem. En teknisk riskanalys har gjorts av Intraservice som enligt dokumentet avser att utgöra underlag till kravställning och formulering av avtalsvillkor avseende informationssäkerhet. Enligt företrädare från utbildningsförvaltningen har inte den tekniska riskanalysens identifierade risker eller åtgärder fastställts eller godkänts av utbildningsförvaltningen.

Vi har tagit del av de informationssäkerhetskrav som ställdes i samband med upphandlingen av IST Administration. Dokumentet är daterat 2017-12-18. Kraven består av 43 punkter inom följande områden: systematiskt informationsarbete, dataskydd, loggning och spårbarhet, autentisering, säkerhetskopiering och återställning, kontinuitetsplanering samt skydd av datorhall. Det framgår vidare av kraven att leverantören för de delar av verksamheten som berörs av leveransen ska ha ett ledningssystem för informationssäkerhet. Ledningssystemet skulle i sin tur baseras på ISO/IEC 27001 eller motsvarande standard.

Avtal med IST som leverantör av systemet IST Administration har tecknats av Göteborgs Stad genom Intraservice[5]. I avtalet med systemleverantören ingår köp av förvaltning och utveckling då systemet driftas av leverantören. I systemansvaret ingår att säkerställa att systemet har en tillräcklig informationssäkerhet samt IT-säkerhet i enlighet med de krav som ställts i upphandling och avtal.

En utsedd projektgrupp har haft ansvar för implementeringsprocessen av IST Administration. Projektet bedrevs fram till och med 2022-07-31 i Intraservice regi. Som en del i projektgruppens arbete genomfördes inför implementeringen av systemet en efterlevnadskontroll av de informationssäkerhetskrav som ställts till leverantören i avtal.

[5] Intraservice är en förvaltning inom staden som levererar interna tjänster till Göteborgs stads olika verksamheter. Exempelvis inom IT. Utveckling, drift och support ingår som delar i många av Intraservice tjänster.

Efterlevnadskontrollen dokumenterades i en rapport, senast reviderad av en representant från Intraservice 2020-01-24. Kontrollen och rapporten beskrivs mer utförligt i avsnitt 3.6.1.

Från 2022-08-01 har projektet överförts från Intraservice till de tre skolförvaltningarna med administrativ placering på utbildningsförvaltningen. Överlämningen till skolförvaltningarna har sin bakgrund i det beslut som fattats av stadsdirektören om att tjänsteområde utbildning från och med 2022-08-01 ska upphöra att vara en kommungemensam intern tjänst. Utbildningsförvaltningen har vid övergång av ansvar även tagit över ansvar för avtal med leverantören av systemet.

Respektive nämnd och förvaltning hade fram till överlämnandet från Intraservice främst arbetat med krav i enlighet med dataskyddsförordningen för IST Administration samt med hantering av personuppgiftsincidenter. Bland annat uppger intervjuade att konsekvensbedömningar gjorts för de personuppgiftsbehandlingar som sker i systemet. Det har även genomförts ett arbete för att säkerställa en säker hantering för elever med skyddade personuppgifter.

Fokus efter överlämningen till förvaltningarna från Intraservice uppges ha varit att ta del av information och underlag från projektgruppen och funktioner inom Intraservice. Ett arbete har påbörjats med att se över systemförvaltningsorganisationen, uppdatera systemförvaltningsplanen och ta fram en plan för informationssäkerhetsarbetet. Arbetet med uppdaterade informationsklassningar, riskanalyser eller efterlevnadskontroller för IST Administration hade vid tiden för granskningen inte påbörjats inom förvaltningarna.

I samband med beslutet att tjänsteområde utbildning skulle överföras till skolnämnderna fick nämnden för Intraservice i uppdrag att överlämna eller överlämna och införliva allmänna handlingar rörande Intraservice verksamhetsområde utbildning till skolnämnderna.

Organisations- och ansvarsfördelningen kring IST Administration, uppges av intervjuade från utbildningsförvaltningen och grundskoleförvaltningen, för tillfället vara något otydlig. Detta med hänvisning till bytet av systemägare från Intraservice till

skolförvaltningarna men även på grund av att implementeringen av systemet i stora delar har slutförts och den projektgrupp som haft huvudansvaret börjat en överlämning till ordinarie förvaltning inom skolförvaltningarna.

3.1.3 Förvaltningsorganisation

I samband med upphandling och avtalstecknande med systemleverantören för IST Administration ingick en förvaltningsplan i dokumentationen. I förvaltningsplanen presenteras en förvaltningsorganisation med en nivåindelning mellan strategisk- taktisk- och operativ nivå där samverkan och forum mellan leverantör och beställare beskrivs. Det framgår av dokumentationen att förvaltningsorganisationen etableras som en del i avvecklingsfasen i införandeprojektet då de föreslagna forumen och roller bemannas.

Intervjuade uppger att den föreslagna förvaltningsorganisationen ännu inte har etablerats men att det är en del i det pågående arbetet inom både utbildningsförvaltningen och grundskoleförvaltningen. Företrädare från utbildningsförvaltningen uppger att de i nuläget arbetar för att etablera nya forum för samverkan med leverantören men att samverkansmodellen ännu inte etablerats fullt ut. Företrädare från grundskoleförvaltningen uppger att de i likhet med utbildningsförvaltningen arbetar med att uppdatera och etablera samverkansmodellen. Deltagare från NAIS-projektet stödjer förvaltningarna i arbetet med att upprätta forum med leverantören. Enligt uppgift så finns inplanerade möten för det operativa forumet för grundskoleförvaltningen med start från slutet av 2022.

Intervjuade från projektgruppen beskriver att kontaktvägar mot leverantören under projektets genomförande främst skett genom projektledare som kommunicerat med motsvarande funktioner hos leverantören. Det uppges ha funnits en tydlig roll- och ansvarsfördelning genom den etablerade projektorganisationen. Det har även funnits en styrgrupp för projektet, där representanter från leverantören, Intraservice och skolförvaltningarna ingick genom rollerna projekt- och systemägare. Projektet pågår fortfarande för de delar som återstår att implementera där projekt- och styrgrupp för

IST Administration bedömt att nuvarande funktionalitet inte är tillräcklig och behöver vidareutvecklas av leverantören innan leveransgodkännande sker och det övergår till ordinarie förvaltning.

Enligt uppgift har det vid tiden för intervjuer i granskningen initierats ett arbete för att etablera en förvaltningsorganisation i enlighet med förvaltningsplanens beskrivning.

3.1.4 Bedömning

Nedan redogörs för vår bedömning kopplad till revisionsfrågan.

Har nämnderna säkerställt att det för IST-administration finns en ändamålsenlig organisation med en tydlig roll-, ansvars-, och befogenhetsfördelning i informationssäkerhetsarbetet?

Vår bedömning är att nämnderna inte vid tiden för granskningen har säkerställt att det för IST-administration finns en ändamålsenlig organisation med en tydlig roll, ansvars- och befogenhetsfördelning i informationssäkerhetsarbetet.

Vi bedömer att informationsägarskapet tydligare behöver etableras i enlighet med interna styrdokument och beslut om ansvar. Detta för att säkerställa att informationssäkerhetsarbetet genomförs inom respektive nämnd med en följsamhet till interna styrdokument och gällande regelverk som nämnderna behöver beakta i sitt informationssäkerhetsarbete.

Vår bedömning är att båda nämnderna saknar etablerade förvaltningsorganisationer så att den ansvarsfördelning som enligt avtal ska gälla mellan skolförvaltningarna och leverantören av IST Administration kan upprätthållas. Detta riskerar att försvåra uppföljning av de informationssäkerhetskrav som ställts och kan försvåra att i tid identifiera behov av relevanta informationssäkerhetsåtgärder.

3.2 Behörighetshantering

Av riktlinjen för informationssäkerhet framgår att åtkomst och behörighet till informationstillgångar ska ges restriktivt och styras av arbetssituation. Särskilt restriktiv ska behörigheten till IT-baserade informationssystem vara. Det ska enligt riktlinjen finnas dokumenterade, formellt beslutade regelverk och arbetssätt gällande på- och avregistrering samt för lösenordstilldelning avseende IT-baserade informationssystem. Det framgår inte av riktlinjen vem eller vilken instans som ska besluta om dessa regelverk.

Varken grundskoleförvaltningen eller utbildningsförvaltningen har i granskningen presenterat dokumenterade och formellt beslutade regelverk för sin behörighetshantering. Vi har tagit del av ett förslag till rutin för behörighetshantering inom utbildningsförvaltningen, som enligt uppgift väntas beslutas av ansvarig systemförvaltare inom kort. Grundskoleförvaltningen har en instruktion om hur behörigheter läggs till och avslutas genom en manual för hantering i stadens serviceportal. Instruktionen är mer av en praktisk handledning än ett regelverk för behörighetshantering.

Det framgår av intervjuer med grundskoleförvaltningen att de vid en genomgång av samtliga tilldelade behörigheter i IST Administration identifierat ett antal konton där medarbetare avslutat sin anställning men där behörigheten till IST Administration fanns kvar. Samma problematik lyfts även i intervju med utbildningsförvaltningen, dock var antalet felaktiga behörigheter färre. Intervjuade uppger att hanteringen med behörigheter inte fullt ut är systematisk i nuläget. Grundskoleförvaltningen har i samband med införandet av IST Administration genomfört ett förbättringsarbete och utvecklat sin behörighetshantering men beskriver samtidigt att den nya rutinen avser att stärka och tydliggöra behörighetshanteringen ytterligare.

I samband med upphandling av systemet ställdes krav på åtkomsthantering till leverantören. Av intervjuer framgår att det i IST Administration finns en väl utvecklad

behörighetsstruktur där åtkomst till information och funktioner i systemet ges utifrån förutbestämda roller, exempelvis om användaren är en elev, lärare eller administratör.

Leverantören av IST Administration har valt att dela upp skolförvaltningarnas data i tre ”instanser” vilket innebär att information inte delas mellan förvaltningarna. Anledningen till det uppges vara att det inte var möjligt att på ett tillräckligt säkert och heltäckande vis separera data i en gemensam instans. Intervjuade uppger att det i nuläget inte finns någon funktion inom skolnämndernas verksamheter med åtkomst till samtliga tre system genom en inloggning.

3.2.1 Bedömning

Nedan redogörs för vår bedömning kopplad till revisionsfrågan.

Har nämnderna säkerställt att det finns rutiner som medför att lämnade behörigheter att ta del av, ändra eller lägga till information i IST- administration är aktuella och korrekta?

Vår bedömning är att grundskolenämnden och utbildningsnämnden inte har etablerat rutiner som medför att lämnade behörigheter för att ta del av, ändra eller lägga till information i IST-administration är aktuella och korrekta. Ingen av nämnderna lever upp till kravet i stadens riktlinje för informationssäkerhet att behörighetsregler ska dokumenteras och beslutas. Utöver det så har felaktiga behörigheter identifierats i tidigare kontroller vilket tyder på bristande rutiner.

Vår bedömning är att systemet i sin uppbyggnad har en integrerad behörighetsstruktur som i stora delar styr vad användare har åtkomst till för information. Att systemet är uppdelat i tre logiskt separerade instanser bidrar även det till en mer restriktiv åtkomst med mindre risk att obehöriga får tillgång till information som de inte har rätt till mellan verksamheter.

3.3 Hantering av skyddade personuppgifter

Ansvariga i implementeringsprojektet av IST Administration har tillsammans med skolförvaltningarna bedömt att nuvarande funktionalitet i systemet inte är tillräckligt säker för att kunna hantera elever med skyddade personuppgifter. Intervjupersonerna uppger att det finns en befintlig lösning för hantering av elever med skyddade uppgifter i systemet, men att leverantören behöver åtgärda ett antal identifierade sårbarheter innan uppgifter om elever med skyddade personuppgifter läggs in i systemet.

Förvaltningarna har i nuläget valt olika arbetssätt för sin hantering av elever med skyddade personuppgifter. Båda förvaltningarna har beslutade rutiner och riktlinjer för sin hantering.

I nuläget hanterar grundskoleförvaltningen dessa uppgifter helt manuellt utanför systemet. Utbildningsförvaltningen har i stället valt att ha en manuell process där uppgifter för elever med skyddad identitet ges en pseudonym och sedan registreras i systemet med de fiktiva uppgifterna. Det innebär att elevens riktiga uppgifter inte hanteras digitalt men att eleven genom sin pseudonym kan finnas i systemet och hanteras som övriga elever.

Intervjupersoner uppger att de har en systematisk hantering av skyddade elevers personuppgifter. Enligt intervjuade är det ett mycket begränsat antal medarbetare som har behörighet att hantera information om elever med skyddade personuppgifter.

Det framgår av intervjuer att det vore önskvärt att kunna ha alla elever i systemet, detta då det finns andra risker med att inte ha alla registrerade. Exempelvis då det inte finns möjlighet till en likvärdig hantering kopplat till verksamhets- och utbildningsprocesser.

3.3.1 Bedömning

Nedan redogörs för vår bedömning kopplad till revisionsfrågan.

Har nämnderna säkerställt att skyddade personuppgifter hanteras på ett sådant sätt att de inte röjs för obehöriga?

Vår bedömning är att både utbildningsnämnden och grundskolenämnden i huvudsak har säkerställt att skyddade personuppgifter hanteras utan att röjas till obehöriga då dessa uppgifter inte hanteras i IST Administration. Då systemet inte bedömts uppnå tillräckliga skyddsnivåer har båda nämnderna valt att ha en manuell hantering av elever med skyddade personuppgifter

Vår bedömning är dock att det finns andra informationssäkerhetsrisker med en manuell hantering som behöver beaktas av nämnderna. Dels risker kopplade till informationens riktighet och spårbarhet, dels risk att elever inte får likvärdiga förutsättningar till information som delges genom digitala systemstöd.

Informationshanteringen för elever med skyddade personuppgifter är av högt skyddsvärde och måste hanteras med erforderliga säkerhetsåtgärder. Vi anser därför att nämnderna, vid tiden när leverantören meddelar att systemet är färdigutvecklat, bör ställa krav på penetrationstest eller andra tekniska tester för att säkerställa att ingen obehörig kan få åtkomst till de uppgifter om elever med skyddade personuppgifter som hanteras i systemet.

3.4 Säkerhetsmonitorering

Enligt avtalade informationssäkerhetskrav för IST Administration framgår att leverantören ska ha dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter.

I en presentation som leverantören genomfört i samband med efterlevnadskontrollen 2019 framgår att de har övervakning dygnet runt, året runt för övervakning och beredskap för IT-infrastruktur. I efterlevnadskontrollen framgår loggning och spårbarhet som områden som inte når ställda informationssäkerhetskrav. Oklarheter har främst avsett loggning och spårbarhet för användare i systemet. Intervjuade uppger dock att det främst är angeläget för spårbarhet för handläggning och inte ur säkerhetssynpunkt.

Det finns ingen uppdaterad efterlevnadskontroll som beskriver hur leverantörens arbete med säkerhetsmonitorering och övervakning fungerar i nuläget. Utredningar har dock gjorts av NAIS-projektet tillsammans med leverantören vilket av intervjuade uppges ha lett fram till samsyn om hur det fortsatta utvecklingsarbetet ska prioriteras för att nå ställda krav för säkerhetsmonitorering och loggning.

Enligt intervjuade finns ett team hos leverantören som löpande utvärderar och bedömer incidenter. Incidentrapporter dokumenteras för samtliga incidenter som inträffat och kommuniceras till kunder via förutbestämda kommunikations- och eskaleringsvägar. I rapporten för efterlevnadskontroll från 2019 framgår behov av att tydliggöra vilka inom Intraservice eller skolförvaltningarna som ska vara mottagare av information vid incidenter i IST Administration.

Logghantering sker i det IST kallar händelseloggen. Intervjupersonerna uppger att de har möjlighet att ta del av säkerhetsloggar på begäran. Tanken är att allt ska loggas i händelseloggen. För en fullständig efterlevnad av informationssäkerhetskraven som ställs anger intervjuade att det finns behov av förbättringar av läsbarhet och användarvänlighet i systemets händelselogg.

3.4.1 Bedömning

Nedan redogörs för vår bedömning kopplad till revisionsfrågan.

Har nämnderna säkerställt att säkerhetsmonitorering inkluderande loggning av säkerhetsrelevanta händelser sker på ett ändamålsenligt sätt i IST-administration?

Vår bedömning är att nämnderna i avtal med leverantören ställt informationssäkerhetskrav för IST Administration som inkluderar säkerhetsmonitorering och loggning av säkerhetsrelevanta händelser. Genom att projektgruppen för systemimplementeringen har identifierat brister i leverantörens förmåga att säkerhetsmonitorera och logga säkerhetsrelevanta händelser pågår ett utvecklingsarbete för att detta ska ske på ett ändamålsenligt sätt i IST Administration.

Vår bedömning är att nämnderna utifrån sitt övergripande ansvar för säkerhetsfrågorna har brustit i kontroller av leverantörens förmåga att övervaka och logga säkerhetshändelser. Detta då ingen uppdaterad efterlevnadskontroll har genomförts sedan 2019 för att säkerställa en ändamålsenlig loggning och övervakning av säkerhetshändelser.

3.5 Kontinuitetshantering och tillhörande backup-rutiner

3.5.1 Kontinuitetsplanering

Av riktlinje för informationssäkerhet framgår att formellt beslutade kontinuitetsplaner ska finnas för verksamheterna. I dessa ska ingå beslut om längsta acceptabla tid som informationssystemet får vara otillgängligt.

Kontinuitetsplaner som inkluderar IT-baserade informationssystem ska omfatta återstarts- och reservrutiner för driftverksamheten som vidtas inom ramen för ordinarie drift så att återstart kan ske inom fastställd tid. Kontinuitetsplanen ska hållas aktuell och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott.

Varken grundskoleförvaltningen eller utbildningsförvaltningen har dokumenterade kontinuitetsplaner för IST Administration. Både förvaltningarna uppger att de har startat ett arbete med att upprätta kontinuitetsplaner.

I efterlevnadskontrollen 2019 framgår att leverantören efterlever krav på kontinuitetsplanering och säkerhetskopiering för IST Administration. Vi har tagit del av underlag från leverantören där bland annat teknisk infrastruktur samt organisatoriska och tekniska kontroller presenteras. Leverantören beskriver i sin dokumentation att de nyttjar en extern part som är expert på datalagring.

Det datacenter som används av IST för IST Administration är certifierat enligt de internationella standarderna ISO 27001 och ISO 22301. Standarden ISO 27001 avser informationssäkerhet och ISO 22301 avser verksamhetens kontinuitet. Genom certifieringen sker årliga externa revisioner av leverantörens efterlevnad av krav enligt ISO. I samband med denna revision har projektledaren för NAIS-projektet begärt in uppdaterade intyg på leverantörens certifieringar. Vi har genom informationssäkerhetssamordnarna inom respektive förvaltning fått del av certifikat som inkommit under november månad 2022. Av certifikatet framgår att leverantören inklusive det datacenter som anlitas som underleverantör uppfyller krav för certifiering. Intyget är gällande till 6 juli 2024.

3.5.2 Backup-rutiner

Av intervjuer med representanter i NAIS-projektet framgår att backup och återläsning av data testats av leverantören för mindre datamängder i samband med driftsstopp och att det har fungerat väl utan förlust av data. Det har dock inte genomförts några större tester där återläsning och verifiering av data gjorts av förvaltningarna eller Intraservice. De intervjuade uppger vidare att de tagit del av dokumentation[6] från leverantören där rutiner för backup av program och data samt återläsning av data finns beskrivet. Därtill finns dokumentation som beskriver hur det datacenter som nyttjas har säkerställt den fysiska säkerheten samt genom redundans och segmentering vidtagit åtgärder för kommunikationssäkerhet.

Intervjupersoner från projektgruppen anger vidare att leverantören på ett trovärdigt och tydligt sätt visat att hanteringen sker på ett korrekt sätt och att det inte finns någon oro över att detta inte ska fungera tillräckligt. Som vi beskrivit tidigare finns ingen ny dokumenterad efterlevnadskontroll där uppföljning av detta gjorts efter 2019.

3.5.3 Bedömning

Nedan redogörs för vår bedömning kopplat till revisionsfrågorna.

Har nämnderna säkerställt att det för IST-administration finns en aktuell, dokumenterad och beslutad kontinuitetsplan?

Har nämnderna säkerställt att det för IST-administration finns tillfredsställande rutiner för backup av program och data, samt för återläsning av data?

Vår bedömning är att nämnderna inte har säkerställt att det finns en aktuell, dokumenterad och beslutad kontinuitetsplan då detta saknas för båda nämnderna vid tiden för granskningen. Leverantören har dokumenterade rutiner och processer för

[6] IST SAAS SERVICES, Operating Environment and Technical Infrastructure, Organizational & Technical controls.

kontinuitetsplanering vilka bedömts efterleva de krav som ställts på leverantören av IST Administration.

I informationssäkerhetskraven för IST Administration ingår krav på rutiner för backup av program och data. Leverantören har genom aktuellt certifieringsintyg uppvisat efterlevnad av certifieringskrav för sitt arbete med lagring och backup. Vår bedömning är att nämnderna endast delvis har följt upp att det finns tillfredsställande rutiner och vi gör därför bedömningen att det finns behov av en mer regelbunden och stärkt kontroll för att säkerställa att den information som ska finnas tillgänglig är säkerhetskopierad och går att återläsa vid behov.

Vår bedömning är även att återläsning av större datamängder som leverantören gör bör testas och verifieras av informationsägarna i både grundskolenämnden och utbildningsnämnden. Detta för att konstatera att ingen information skadats eller förlorats vid återläsning. Att detta behöver göras kan med fördel specificeras i de kontinuitetsplaner som ska upprättas. Dessa bör testas regelbundet så att den dokumenterade planeringen skulle fungera ändamålsenligt i händelse av en allvarligare störning eller avbrott.

3.6 Uppföljning av informationssäkerhetsnivå IST Administration

I riktlinjen för informationssäkerhet regleras att verksamhetens ledning kontinuerligt ska följa upp att säkerhetsnivån är acceptabel och uppföljning av informationssäkerhetsnivån i form av intern kontroll ska ske minst årligen. Resultatet ska rapporteras till nämnden.

I riktlinjen framgår även att efterlevnad av säkerhetsrutiner och aktuella regler behöver säkerställas under hela informationssystemets livscykel. Vidare anges att IT-baserade informationssystem ska analyseras regelbundet för identifiering av sårbarheter eller annan problematik som riskerar orsaka incidenter.

Som vi beskrivit tidigare i rapporten har en efterlevnadskontroll av informationssäkerhetskraven som ingår i avtal för IST Administration genomförts 2019-12-05 av representanter från projektgruppen och Intraservice. Intraservice har därtill i samråd med leverantören genomfört penetrationstest för att utvärdera skyddsnivåer i IST Administration ett flertal gånger. Resultatet av de tekniska testerna har hanterats och åtgärdats av Intraservice i samarbete med leverantören.

Intervjuade uppger att varken grundskoleförvaltningen eller utbildningsförvaltningen har genomfört någon uppföljning eller kontroll av informationssäkerhetsnivån efter övertagandet av ansvar för IST Administration 2022.

Vi har i granskningen tagit del av internkontrollplaner 2022 för utbildningsnämnden och för grundskolenämnden. Av dokumentgranskning kan vi konstatera att de kontrollområden som ingår i planerna till viss del inkluderar informationssäkerhet och system, men inte specifikt informationssäkerhetsrisker för IST Administration.

Av protokollsgenomgång noterar vi att den rapportering som har skett till utbildningsnämnden och grundskolenämnden under 2022 främst har avhandlat funktionalitetsbrister i IST Administration och inte redogjort för informationssäkerhetsnivå eller tillhörande risker i systemet.

3.6.1 Bedömning

Nedan redogörs för vår bedömning kopplad till revisionsfrågan.

Har nämnderna säkerställt att informationssäkerhetsnivån i IST- administration löpande är acceptabel, att den följs upp årligen och att nämnden erhåller en rapport av resultaten av denna uppföljning?

Vår bedömning är att nämnderna inte har säkerställt att informationssäkerhetsnivån i IST-administration löpande är acceptabel. Informationsklassning har inte gjorts för den information som hanteras i systemet av respektive nämnds verksamheter och det har inte skett någon årlig uppföljning och rapportering till nämnderna med information om informationssäkerhetsnivån för systemet. Risker som ingår i internkontrollplan för 2022 berör till viss del informationssäkerhetsområdet men vår bedömning är att denna kontroll inte är tillräcklig.

Informationsklassning, teknisk riskanalys och efterlevnadskontroll har i huvudsak gjorts av Intraservice och inom NAIS-projektet innan systemet implementerades. Penetrationstest har gjorts i syfte att analysera sårbarheter eller annan problematik som riskerar orsaka incidenter efter initiativ från Intraservice. De aktiviteter som genomförts för att utvärdera informationssäkerhetsnivån för IST Administration har inte genomförts som en del i nämndernas systematiska informationssäkerhetsarbete i syfte att skydda informationstillgångar som nämnderna ansvarar för. Vår bedömning är att nämnderna som övergripande ansvariga för säkerheten har brustit i sitt ansvar för informationssäkerheten då aktiviteter i enlighet med beslutade riktlinjer för informationssäkerhet inte har genomförts.

Den efterlevnadskontroll som genomfördes 2019 påvisar en hög grad av kontrollmoment och dokumenterade underlag som till stor del verifierar att leverantören uppfyller krav. Vår bedömning är att liknande kontroller bör genomföras regelbundet och att dokumentation inhämtas som verifierar att leverantören upprätthåller en tillräcklig informationssäkerhet för systemet i enlighet med ställda krav.

4 Sammanfattande bedömning

Vår sammanfattande bedömning utifrån granskningens syfte är att nämnderna endast delvis bedriver ett informationssäkerhetsarbete som säkerställer konfidentialitet, riktighet och tillgänglighet i de informationstillgångar som hanteras i det skoladministrativa systemstödet IST-administration.

Vid tiden för granskningen har nämnderna inte säkerställt att det för IST-administration finns en ändamålsenlig organisation med en tydlig roll, ansvars- och befogenhetsfördelning för informationssäkerhetsarbetet. Informationsägarskapet behöver tydliggöras och etableras i enlighet med interna styrdokument och beslut om ansvar.

Grundskolenämnden och utbildningsnämnden har inte i tillräcklig grad säkerställt en efterlevnad av riktlinje för informationssäkerhet. Exempelvis har inte informationsägaren tillsett att informationsklassning och tillhörande riskanalyser gjorts för den information som hanteras i IST Administration. Det finns därigenom en risk att information inte skyddas med erforderliga tekniska och administrativa skyddsåtgärder.

Nämnderna saknar etablerade förvaltningsorganisationer så att den ansvarsfördelning som enligt avtal ska gälla mellan skolförvaltningarna och leverantören av IST Administration kan upprätthållas. Detta riskerar att försvåra uppföljning av de informationssäkerhetskrav som ställts och kan försvåra att i tid identifiera behov av relevanta informationssäkerhetsåtgärder.

Båda nämnderna har i sitt personuppgiftsansvar analyserat risker genom konsekvensbedömningar för de personuppgiftsbehandlingar som hanteras i IST Administration. Genom det har åtgärder kunnat vidtas för att skydda personuppgifter som hanteras i systemet. Beslut har exempelvis fattats att uppgifter om elever med skyddade personuppgifter inte kan hanteras i systemet då detta uppfattas alltför sårbart med nuvarande funktionalitet. Särskilda rutiner har fastställts inom båda nämnderna för en manuell hantering av dessa uppgifter till dess att systemet är utvecklat och bedömts

som tillräckligt säkert för att lägga in uppgifter om elever med skyddade personuppgifter. Vår bedömning är dock att det finns andra informationssäkerhetsrisker med en manuell hantering som behöver beaktas av nämnderna. Dels risker avseende informationens riktighet och spårbarhet, dels risker kopplade till elevers förutsättningar att på likvärdiga sätt erhålla information och ha en tillgänglig dokumentation avseende studier och skolverksamhet.

Grundskolenämnden och utbildningsnämnden har inte etablerat rutiner som medför att lämnade behörigheter för att ta del av, ändra eller lägga till information i IST-administration är aktuella och korrekta. Ingen av nämnderna lever upp till kravet i stadens riktlinje för informationssäkerhet att behörighetsregler ska dokumenteras och beslutas. Vi bedömer att systemet i sin uppbyggnad har en integrerad behörighetsstruktur som i stora delar styr vad användare har åtkomst till för information vilken baseras på förutbestämda roller och vilken enhet som användare tillhör.

Nämnderna har genom avtalade informationssäkerhetskrav för IST Administration inkluderat säkerhetsmonitorering inkluderande loggning av säkerhetsrelevanta händelser. Genom att projektgruppen för systemimplementeringen har identifierat brister i leverantörens förmåga att säkerhetsmonitorera och logga säkerhetsrelevanta händelser pågår ett utvecklingsarbete för att detta ska ske på ett ändamålsenligt sätt i IST Administration. Vår bedömning är att nämnderna utifrån sitt övergripande ansvar för säkerhetsfrågorna har brustit i kontroller av leverantörens förmåga att övervaka och logga säkerhetshändelser. Detta då ingen uppdaterad efterlevnadskontroll har genomförts sedan 2019 för att säkerställa att loggning och övervakning av säkerhetshändelser sker på ett ändamålsenligt sätt.

Vår bedömning är att nämnderna inte har säkerställt att det finns en aktuell, dokumenterad och beslutad kontinuitetsplan då detta saknas för båda nämnderna vid tiden för granskningen. Leverantören har dokumenterade rutiner och processer för kontinuitetsplanering vilka bedömts efterleva de krav som ställts på leverantören av IST Administration.

I informationssäkerhetskraven för IST Administration ingår krav på rutiner för backup av program och data. Leverantören har genom aktuellt certifieringsintyg uppvisat efterlevnad av certifieringskrav för sitt arbete med lagring och backup. Vår bedömning är att nämnderna endast delvis har följt upp att det finns tillfredsställande rutiner och vi gör därför bedömningen att det finns behov av en mer regelbunden och stärkt kontroll för att säkerställa att den information som ska finnas tillgänglig är säkerhetskopierad och går att återläsa vid behov.

Vår bedömning är dock att återläsning av större datamängder behöver testas och verifieras av informationsägarna i både grundskolenämnden och utbildningsnämnden för att konstatera att ingen information skadats eller förlorats vid en återläsning.

Slutligen är vår bedömning att nämnderna inte har säkerställt att informationssäkerhetsnivån i IST-administration löpande är acceptabel. Informationsklassning har inte gjorts för den information som hanteras i systemet av respektive nämnds verksamheter och det har inte skett någon årlig uppföljning och rapportering till nämnderna med information om informationssäkerhetsnivån för systemet. Risker som ingår i internkontrollplan för 2022 berör till viss del informationssäkerhetsområdet men vår bedömning är att denna kontroll inte är tillräcklig.

Datum som ovan

KPMG AB

Jenny Thörn

Kommunal revisor

Projektledare

David Bäcker

Certifierad kommunal revisor

Kvalitetssäkrare KPMG