Härnösands kommuns revisorer

Till
Kommunstyrelsen

För kännedom:
Kommunfullmäktige

2026-04-09

Revisionsrapport ”Uppföljande granskning av IT-säkerhet”

Azets har på uppdrag av kommunens revisorer genomfört en uppföljning av tidigare granskning av IT-säkerhet. Uppdraget ingick i revisionsplanen för år 2025.

Revisionen ser allvarligt på att tillräckliga åtgärder inte har vidtagits utifrån tidigare rekommendationer.

Revisionen önskar att kommunstyrelsen lämnar synpunkter på de slutsatser som finns redovisade i rapporten senast den 14 augusti 2026. Av svaret bör det framgå vilka eventuella åtgärder som ska vidtas och när de beräknas vara genomförda.

Svaret skickas till Lena Medin, Azets (mailadress lena.medin@azets.com) för vidarebefordran till revisorerna.

För Härnösands kommuns revisorer

Maria Öberg
Ordförande

Lillemor Andersson
1:e vice ordförande

Uppföljande granskning av IT-säkerhet

Rapport

Härnösands kommun

2026-04-09

Antal sidor: 13

INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING

Azets Revision & Rådgivning har av Härnösands kommuns revisorer fått i uppdrag att översiktligt följa upp tidigare granskning av IT-säkerhet.

Syftet med granskningen har varit att bedöma om åtgärder har vidtagits i enlighet med de rekommendationer som lämnades och enligt kommunstyrelsens svar.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen endast delvis vidtagit åtgärder i enlighet med de rekommendationer som lämnats.

Bakgrunden till vår samlade bedömning är att kommunen under år 2023 har antagit styrdokument för informationssäkerhet, men att dessa kommer att behöva revideras till följd av ny lagstiftning under år 2026.

Det saknas en kvalitativ utvärdering av hur resurserna för informationssäkerhetsarbetet är fördelade, vilket innebär att prioriteringar och åtgärder ännu inte kunnat genomföras.

Vidare sker en årlig uppföljning till kommunledningsgruppen, men denna omfattar endast vissa delar och ger därmed inte en helhetsbild av kommunens samlade informationssäkerhetsarbete. Kommunen tillhandahåller utbildningar via intranätet, men dessa är varken obligatoriska eller möjliga att följa upp systematiskt. Motsvarande utbildningar för förtroendevalda saknas. Dock framgår att ett arbete med att systematisera utbildningserbjudandet pågår genom att göra vissa delar obligatoriska och möjliga att följa upp.

När det gäller incidenthantering visar granskningen att det finns information om hur personuppgiftsincidenter ska rapporteras, men att kommunen saknar formaliserade och sammanhållna rutiner med tydliga roller, ansvar, processer och eskaleringsvägar. Incidentrapporteringen sker huvudsakligen via e-post. Det saknas ett systematiskt arbetssätt eller central logg för registrering, kategorisering och uppföljning av incidenter.

I det följande redovisas våra samlade bedömningar av respektive revisionsfråga.

Revisionsfråga	Bedömning
Har riktlinjer för informationssäkerhet aktualiserats och har en bedömning skett avseende behov av revidering?	I allt väsentligt
Har en utvärdering av resursfördelning för informationssäkerhetsarbetet inklusive IT-säkerhetsåtgärder vidtagits och är de tillräckliga i förhållande till behov och risker?	Nej
Sker en samlad uppföljning av informationssäkerhetsarbetet i enlighet beslutade riktlinjer?	Endast delvis
Har utbildningsinsatser etablerats inom informationssäkerhet, inkluderat IT-säkerhet, för medarbetare och förtroendevalda? Är insatserna regelbundna och kan de följas över tid?	Endast delvis/Nej
Finns incidenthanteringsrutiner med tydliggjorda eskaleringsvägar för att i tid ha förutsättningar att upptäcka och agera på incidenter?	Endast delvis
Finns logg och uppföljning av inträffade incidenter?	Nej

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen att:

- Säkerställa att *Riktlinje för informationssäkerhet* revideras utifrån nu gällande lagstiftning.
- Säkerställa att en utvärdering av resursfördelning för informationssäkerhetsarbetet, inklusive IT-säkerhetsåtgärder, genomförs och att tillräckliga åtgärder vidtas vid behov.
- Säkerställa att en samlad uppföljning av informationssäkerhet genomförs minst en gång per år.
- Etablera formaliserade och heltäckande rutiner för incidenthantering, som omfattar tydliggjorda eskaleringsvägar.
- Säkerställa att registrering och uppföljning av inträffade incidenter genomförs systematiskt.
- Säkerställa att utbildningsinsatser inom området genomförs strukturerat, samt att deltagande följs upp.

2 BAKGRUND

Azets Revision & Rådgivning har av Härnösands kommuns revisorer fått i uppdrag att översiktligt följa upp tidigare granskning av IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2025.

Revisorerna bedömer att det finns en risk att tillräckliga åtgärder inte har vidtagits utifrån de rekommendationer som lämnades.

3 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

Granskningen har syftat till att bedöma om åtgärder har vidtagits i enlighet med de rekommendationer som lämnade och enligt kommunstyrelsens svar.

Granskningen har omfattat följande revisionsfrågor:

- Har Riktlinjer för informationssäkerhet aktualiserats och har en bedömning skett avseende behov av revidering?
- Har en utvärdering av resursfördelning för informationssäkerhetsarbetet inklusive IT-säkerhetsåtgärder vidtagits och är de tillräckliga i förhållande till behov och risker?
- Sker en samlad uppföljning av informationssäkerhetsarbetet i enlighet beslutade riktlinjer?
- Har utbildningsinsatser etablerats inom informationssäkerhet, inkluderat IT-säkerhet, för medarbetare och förtroendevalda? Är insatserna regelbundna och kan de följas över tid?
- Finns incidenthanteringsrutiner med tydliggjorda eskaleringsvägar för att i tid ha förutsättningar att upptäcka och agera på incidenter?
- Finns logg och uppföljning av inträffade incidenter?

3.1 AVGRÄNSNING OCH ANSVARIG STYRELSE

Granskningen har varit översiktlig.

4 REVISIONSKRITERIER

I granskningen har revisionskriterierna utgjorts av:

- 6 kap. 6 § kommunallagen (2017:725), KL

5 METOD

Granskningen har genomförts genom:

- Dokumentstudier av erhållna styrande och stödjande dokument.
- Intervju och skriftlig avstämning med kanslichef och informationssäkerhetssamordnare.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.

Rapporten är faktakontrollerad av kanslichef och informationssäkerhetssamordnare.

6 RESULTAT AV GRANSKNINGEN

6.1 RIKTLINJER OCH UPPFÖLJNING

I detta avsnitt besvaras följande revisionsfrågor:

- Har riktlinjer för informationssäkerhet aktualiserats och har en bedömning skett avseende behov av revidering?
- Har en utvärdering av resursfördelning för informationssäkerhetsarbetet inklusive IT-säkerhetsåtgärder vidtagits och är de tillräckliga i förhållande till behov och risker?
- Sker en samlad uppföljning av informationssäkerhetsarbetet i enlighet beslutade riktlinjer?

Rekommendation

I den tidigare granskningen från 2022 rekommenderades kommunstyrelsen att aktualisera *Riktlinjer för informationssäkerhet* och samtidigt göra en bedömning om det finns behov av revidering.

Därtill rekommenderades kommunstyrelsen att utvärdera om nuvarande resursfördelning för informationssäkerhetsarbetet inklusive IT-säkerhetsåtgärder är tillräcklig i förhållande till behov och risker.

Kommunstyrelsen rekommenderades även att etablera en samlad uppföljning av informationssäkerhetsarbetet i enlighet med beslutade riktlinjer. Detta för att säkerställa en efterlevnad av styrande dokument och att väsentliga aktiviteter som riskbedömning och informationsklassning kan utgöra underlag för tekniska åtgärder som står i relation till skyddsvärdet.

Yttrande

Kommunen delar och tar till sig revisionens rekommendation att aktualisering av nuvarande riktlinjer är nödvändiga samt att komplettera med andra kommunövergripande styrande dokument inom informationsförvaltning.

Kommunen delar och tar till sig revisionens rekommendation. Det är för kommunen en viktig och prioriterad men kostnadsdrivande fråga och är en del av det systematiska arbetet med informations- och IT-säkerhetsarbetet.

Kommunen tar till sig rekommendationerna och kommer att implementera informationssäkerhet i kommunledningens årshjul med en löpande ledningsgenomgång med aktuell lägesbild över bland annat efterlevnad av styrande dokument, riskbedömning och arbetet med informationsklassning.

Nuläge

Ny policy för informationssäkerhet och personuppgiftsbehandling beslutades av kommunfullmäktige 2023-11-11. En ny riktlinje för informationssäkerhet och personuppgiftsbehandling beslutades av kommunstyrelsen 2024-02-27. Kommunens riktlinjer på området har inte reviderats efter detta.

Policyn innehåller Härnösands kommuns viljeriktning och övergripande principer gällande informationssäkerhet och dataskydd. Policyn med kompletterande riktlinjer ska tillämpas i alla situationer där Härnösands kommun och de kommunala bolagen hanterar information med eller utan personuppgifter.

Av intervju framgår att med hänsyn till Cybersäkerhetslagen och aviserade nya föreskrifter under år 2026 bedöms en revidering som nödvändig för att säkerställa efterlevnad och aktualitet. Arbetet med att planera för denna revidering uppges ha påbörjats, men inga beslut har ännu fattats. Därtill nämns att en AI-policy har beslutats av kommunledningsgruppen och förväntas gå upp för beslut i kommunfullmäktige inom närtid.

Av intervju framgår vidare att en kvalitativ utvärdering av nuvarande resursfördelning inom informationssäkerhetsområdet ännu inte genomförts. Cybersäkerhetskollen[1] pekar dock tydligt på behovet av resursförstärkning, särskilt för att möta både ökade krav och nya hotbilder. Detta har identifierats som en prioriterad fråga framgent. Därtill framgår att en IT-säkerhetsansvarig har tillsatts som en del i arbetet att öka IT-säkerhetsförmågan och efterlevnad av Cybersäkerhetslagen.

Av *Policy för informationssäkerhet* framgår att kommunstyrelsen ansvarar för att leda, samordna och följa upp det systematiska arbetet med informationssäkerhet och dataskydd minst en gång per år. Av intervju framgår att en uppföljning av informationssäkerhet genomförs en gång per år till kommunledningsgruppen. Detta är dock ingen samlad uppföljning av informationssäkerhetsarbetet utan behandlar viktiga punkter som anses behövas informeras om inom kommunledningsgruppen. Av den senaste uppföljningen från februari 2026 behandlade uppföljningen implementationen av Cybersäkerhetslagen. I uppföljningen noteras ett urval av åtgärder för detta av cybersäkerhetslagen samt status. Bland annat framgår att obligatorisk utbildning för ledning och ledningsgrupper ska ske, samt åtgärder avseende incidenthanteringsprocessen.

Utöver ovan nämnda uppföljning sker ingen ytterligare uppföljning. Dock nämns att denna typ av uppföljning planeras att framgent rapporteras till kommunstyrelsen.

[1] Cybersäkerhetskollen är samlingsnamnet för Myndigheten för civilt försvars cybersäkerhetsmätningar som mäter nivån på verksamhetens systematiska cybersäkerhetsarbete, samt ger stöd för förbättringsarbete.

6.1.1 Bedömning

Vår bedömning är att det riktlinjer för informationssäkerhet **i allt väsentligt** har aktualiserats och att en bedömning skett avseende behov av revidering.

Bedömningen baseras på att det under år 2023 antagits nya styrdokument för informationssäkerhet. Noteras dock att det uppmärksammats ett behov av revidering av dessa med anledning av ny lagstiftning som kommer att införas under år 2026.

Vår bedömning är att det **inte** skett en utvärdering av resursfördelning för informationssäkerhetsarbetet, samt att det **inte** vidtagits åtgärder.

Vår bedömning baseras på att det inte skett en kvalitativ utvärdering av resursfördelningen. Med anledning av detta har det heller inte vidtagits några åtgärder.

Vår bedömning är att det **endast delvis** sker en samlad uppföljning av informationssäkerhetsarbetet i enlighet med beslutade riktlinjer.

Bedömningen baseras på att det sker en uppföljning till kommunledningsgruppen en gång per år, men denna omfattar inte informationssäkerhetsarbetet i stort utan omfattar endast vissa delar. Dock ser vi positivt på att kommunledningen genomför en uppföljning där åtgärder presenteras. Därtill baseras bedömningen på att kommunstyrelsen inte erhållit någon samlad uppföljning på området.

6.2 UTBILDNINGSINSATSER

I detta avsnitt besvaras följande revisionsfrågor:

- Har utbildningsinsatser etablerats inom informationssäkerhet, inkluderat IT-säkerhet, för medarbetare och förtroendevalda? Är insatserna regelbundna och kan de följas över tid?

Rekommendation

I den tidigare granskningen rekommenderades kommunstyrelsen att etablera utbildningsinsatser inom informationssäkerhet, som inkluderar IT-säkerhet, för medarbetare och förtroendevalda som är återkommande och kan följas upp över tid.

Yttrande

Kommunen instämmer med rekommendationen och planerar att implementera en målgruppsinriktad utbildning under år 2023.

Nuläge

Av tidigare svar till revisionen[2] framgår att en cybersäkerhetsövning har genomförts vid IT-avdelningen den 2023-10-11 och en uppföljning gjordes tillsammans med krisledningen 2023-10-23. Syftet med övningen var att träna incidenthantering och eskaleringsvägar.

Kommunens medarbetare har tillgång till olika utbildningar via intranätet. Enligt genomförda intervjuer är utbildningarna dock inte obligatoriska, utan medarbetarna uppmanas att genomföra dem på frivillig basis. Utbildningarna omfattar informationssäkerhet, dataskydd (GDPR) och säkerhetsmedvetenhet. Däremot nämns vid intervju att dessa kurser från och med 1 april 2026 ska ingå som obligatoriska baskunskaper för alla medarbetare. Det framgår även att utbildning inom cybersäkerhet för kommunens ledning blivit lagstadgad från och med den 15 januari 2026[3], vilket innebär att rutiner och uppföljningsprocesser behöver anpassas. Detta arbete pågår i samverkan med kommunledningsgruppen.

Det framgår av tidigare svar till revisionen[4] att utbildningsmaterial ska finnas tillgängliga för förtroendevalda från och med år 2024 och att förtroendevalda har tillgång till information om IT-säkerhet. Av information från intervjuade framgår att en utbildningskatalog för nämnder skickats ut för nämnderna att boka in olika utbildningsinsatser, men där ingen nämnd har bokat in informationssäkerhet specifikt. I övrigt så följde kommunstyrelsen upp informationssäkerhet i sin uppsikt över nämnderna år 2022, med frågor som rörde styrning/kontroll/kunskaper/resurser/hur man arbetar med incidenter och hur de identifierar potentiella risker.

[2] Uppföljande frågor om samhällsviktig verksamhet och IT-säkerhet under 2023, tjänsteskrivelse 2024-04-19
[3] Den nya cybersäkerhetslagen trädde i kraft den 15 januari 2026. Lagen implementerar det så kallade NIS2-direktivet, som syftar till att uppnå en gemensamt högre nivå av cybersäkerhet inom EU. Allt fler verksamheter faller nu in under cybersäkerhetslagstiftningens tillämpningsområde och omfattas därför bland annat av kraven på anmälningsplikt, incidentrapportering och genomförande av säkerhetsåtgärder.
[4] Uppföljande frågor om samhällsviktig verksamhet och IT-säkerhet under 2023, tjänsteskrivelse 2024-04-19

Av intervju framgår att HR för närvarande arbetar med att utveckla ett systemstöd där både medarbetare och chefer ska kunna följa upp genomförda utbildningar. Systemstödet är ännu inte infört, vilket innebär att kommunen i dagsläget saknar möjlighet att systematiskt följa upp utbildningsdeltagande. Av information från intervjuade framgår att detta kommer finnas på plats den 1 april 2026.

6.2.1 Bedömning

Vår bedömning är att det **endast delvis** finns etablerade utbildningsinsatser inom informationssäkerhet för medarbetare och förtroendevalda. Vidare bedömer vi att insatserna **inte** är regelbundna och kan följas över tid.

Bedömningen grundar sig på att kommunen tillhandahåller utbildningar inom informationssäkerhet via intranätet, men att dessa inte är obligatoriska och inte heller kan följas upp systematiskt. Dock framgår att det pågår ett arbete med att göra vissa delar obligatoriska och möjliga att följa upp.

6.3 Incidenthantering och uppföljning

I detta avsnitt besvaras följande revisionsfrågor:

- Finns incidenthanteringsrutiner med tydliggjorda eskaleringsvägar för att i tid ha förutsättningar att upptäcka och agera på incidenter?
- Finns logg och uppföljning av inträffade incidenter?

Rekommendation

I den tidigare granskningen rekommenderades kommunstyrelsen att etablera incidenthanteringsrutiner med tydliggjorda eskaleringsvägar för att i tid ha förutsättningar att upptäcka och agera på incidenter, samt etablera en logg och uppföljning av inträffade incidenter.

Yttrande

Kommunen instämmer med rekommendationen och har initierat olika initiativ inom området lokalt som regionalt. Kommunen ser att detta är kostnadsdrivande åtgärder som bör prioriteras.

Nuläge

Vi har inte erhållit några skriftliga rutiner eller dokument som beskriver incidenthanteringsprocessen och tydliggör eskaleringsvägar. Den information som lämnats består av en skärmdump från intranätet där det framgår hur en personuppgiftsincident ska rapporteras. Där framgår att i dagsläget sker incidentrapportering via e-post, där medarbetaren med egna ord beskriver händelsen eller misstanken om fel. Därefter gör sakkunniga en bedömning av det rapporterade och vidtar eventuella åtgärder. Enligt intervju saknas i övrigt fastställda rutiner och eskaleringsvägar inom den ordinarie

linjeorganisationen. Ett arbete med att ta fram förslag på nya rutiner pågår på uppdrag av kommundirektören.

På intranätet finns även information om att medarbetare själva, om de utan stöd kan bedöma att en incident uppstått där personuppgifter röjts, kan rapportera en detta till Integritetsmyndigheten (IMY) via myndighetens e-tjänst. En kopia av anmälan ska då diarieföras hos kommunen.

För större händelser finns en etablerad TIB-funktion (tjänsteman i beredskap), som enligt uppgift fungerar som första instans vid incidenter. Därtill lyfts att upphandling av en extern part för hantering av allvarligare incidenter kommer att bli klar under år 2026.

Det finns ingen logg eller samlad uppföljning av inträffade incidenter. Eftersom rapporteringen sker via e-post finns i dagens system ingen möjlighet att få en helhetsbild över inträffade incidenter.

6.3.1 Bedömning

Vår bedömning är att det **endast delvis** finns tydliga incidenthanteringsrutiner med tydliggjorda eskaleringsvägar för att i tid ha förutsättningar att upptäcka och agera på incidenter.

Bedömningen grundas på att kommunen har viss information om hur incidenter ska rapporteras, men att det saknas heltäckande och formaliserade incidenthanteringsrutiner med tydliga eskaleringsvägar. Den information som finns tillgänglig på intranätet beskriver främst hur en personuppgiftsincident anmäls, exempelvis via en e-postadress, men motsvarar inte en sammanhållen rutin som reglerar ansvar, processflöde, roller eller tidiga åtgärder.

Vår bedömning är att det **inte** finns någon logg och uppföljning av inträffade incidenter.

Bedömningen grundas på att kommunen i dagsläget saknar ett systematiskt arbetssätt för att dokumentera och följa upp inträffade incidenter. Incidentrapporteringen sker huvudsakligen via e-post, och det finns ingen central logg eller funktion i nuvarande system som möjliggör samlad registrering, kategorisering eller uppföljning av incidenter över tid. Detta försvårar även arbetet med att kunna upptäcka trender i rapporterade incidenter.

7 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

Syftet med granskningen har varit att bedöma om åtgärder har vidtagits i enlighet med de rekommendationer som lämnade och enligt kommunstyrelsens svar.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen endast delvis vidtagit åtgärder i enlighet med de rekommendationer som lämnats.

Se inledning samt respektive rapportkapitel för en mer detaljerad beskrivning.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen att:

- Säkerställa att *Riktlinje för informationssäkerhet* revideras utifrån nu gällande lagstiftning.
- Säkerställa att en utvärdering av resursfördelning för informationssäkerhetsarbetet, inklusive IT-säkerhetsåtgärder, genomförs och att tillräckliga åtgärder vidtas vid behov.
- Säkerställa att en samlad uppföljning av informationssäkerhet genomförs minst en gång per år.
- Etablera formaliserade och heltäckande rutiner för incidenthantering, som omfattar tydliggjorda eskaleringsvägar.
- Säkerställa att registrering och uppföljning av inträffade incidenter genomförs systematiskt.
- Säkerställa att utbildningsinsatser inom området genomförs strukturerat, samt att deltagande följs upp.

Datum som ovan
Azets Revision & Rådgivning AB

Joakim Hackström-Larsson
Verksamhetsrevisor

Elina Lundberg
Verksamhetsrevisor

Lena Medin
Certifierad kommunal revisor

PENNEO

Signaturerna i detta dokument är juridiskt bindande. Dokumentet är signerat genom Penneo™ för säker digital signering. Tecknarnas identitet har lagrats, och visas nedan.

"Med min signatur bekräftar jag innehållet och alla datum i detta dokumentet."

ELINA LUNDBERG
Verksamhetsrevisor
Serienummer: 16c9893c2d3295[…]f3c00762a8a04
IP: 83.233.xxx.xxx
2026-04-13 08:36:23 UTC

LENA MEDIN
Certifierad kommunal revisor
Serienummer: fdca59a9db67cf[…]85981c060041a
IP: 217.209.xxx.xxx
2026-04-13 08:36:39 UTC

Karin Maria Öberg
Ordförande
Serienummer: 4706b11107cc72[…]29245d00a2a3f
IP: 94.234.xxx.xxx
2026-04-13 09:03:35 UTC

LILLEMOR ANDERSSON
1:e vice ordförande
Serienummer: 3cc6d575497e62[…]328db561f9d78
IP: 95.203.xxx.xxx
2026-04-13 12:54:47 UTC

Joakim Hackström Larsson
Verksamhetsrevisor
Serienummer: 285ca3512a48bf[…]7db8136a1b3f1
IP: 93.92.xxx.xxx
2026-04-15 07:32:18 UTC