Uppföljning av internkontrollplan - helår 2025

Regionstyrelsen

Helår 2025

Region Halland

Innehållsförteckning

1 Sammanfattning

Regionstyrelsens internkontrollplan för år 2025 har innefattat kontroller gjorda inom upphandling, ekonomi, informationssäkerhet samt ledning- och styrning. Samtliga risker har kontrollerats och de risker som kräver åtgärd hanteras vidare.

Sammanfattningsvis när det gäller kontrollerna sticker ett par kontroller ut, dessa kontroller har även lyft fram åtgärder som en följd av resultatet. Kontroll av order som går via e-handel redovisar att stickprover har genomförts och det har funnits vissa avvikelser inom dentala förbrukningsprodukter som har korrigerats. Det har även funnits avvikelser i tolkförmedlingsavgifter som utreds vidare av förvaltningen.

Inom risk för cyberattacker (IT-system) har kontroller genomförts för att säkerställa att kontinutietsplaner är aktuella och övas på. Resultatet visar att manuella kontroller och sårbarhetsuppdateringar sker kontinuerligt, och att automatiserad sårbarhetsanalys har införts. Löpande sårbarhetsskanningar genomförs mot samtliga servrar, inklusive de som är exponerade mot internet. Resultaten av dessa skanningar rapporteras månadsvis till ansvariga.

Vidare har flera kontroller gjorts inom områden styrning och ledning genom bland annat kontroll av att politiska beslut verkställs och risk att statliga uppdrag inte genomförs, där resultatet visar att det inte finns behov av några åtgärder.

2 Uppföljning av kontrollmoment

2.1 Risk med driftstörningar

Kontrollmoment	Resultat av genomförd kontroll
Risk att äldre icke förvaltade system, gammal hårdvara ökar antal driftstörningar. ***Beskrivning av metod**: Antal Windows klienter som är för gamla, Antal operativsystem på servrar som är för gamla och antal databasversioner som är för gamla - två gånger per år*	**Kontrollen är genomförd** Under 2025 har Region Halland fortsatt att minska riskerna kopplade till äldre och icke förvaltade IT-system. Rutiner för livscykelhantering fungerar väl, men efterlevnaden varierar och flera system och plattformar ligger kvar på operativsystem och databasversioner som saknar eller snart förlorar support. Totalt finns ett betydande antal äldre serverplattformar samt databaser som måste uppgraderas senast 2026. På klientsidan har utfasningen av Windows 10 försvårats av att många applikationer – särskilt medicintekniska – ännu inte är verifierade för Windows 11. Detta blockerar migreringen för över 680 datorer och riskerar ökade supportkostnader. Arbetet med att minska antalet icke förvaltade system har gett goda resultat, men skugg-IT i form av okända molntjänster kvarstår som risk. Sammantaget bedöms risken som **delvis hanterad**, men fortsatt väsentlig. Prioriterade områden framåt är utfasning av gamla plattformar, uppgradering av databaser, accelererad applikationsvalidering och förstärkt styrning mot leverantörer och verksamheter.

2.2 Risk för välfärdsbrott

Kontrollmoment	Resultat av genomförd kontroll
Skapa struktur för hur regionkontoret samlat arbetar med att kunskapshöja, medvetandegöra och motverka välfärdsbrottslighet. ***Beskrivning av metod*** *Arbeta kunskapshöjande genom att delta i nationella nätverksmöten och sprida kunskap i berörda sammanhang. På så sätt ökar medvetenheten i organisationen kring välfärdsbrottslighet.* *Skapa en tydlig struktur och effektiv process för hur Region Halland arbetar systematiskt för att motverka välfärdsbrottslighet.*	**Kontrollen är genomförd** Under 2024 initierades Region Hallands arbete med att skapa en struktur för att förebygga och motverka välfärdsbrottslighet. Under 2025 har en struktur för regionkontorets arbete mot välfärdsbrottslighet etablerats, och inom ramen för det arbetet har en nulägesbild och tillhörande handlingsplan med åtgärder tagits fram. Arbetet med att åtgärda identifierade riskområden kommer fortsätta under 2026. Ett arbete har även gjorts med att förstärka perspektivet i de riskanalyser som genomförts under 2025 i Region Halland. Dessa kommer ligga till grund för genomförandet av en regional riskanalys om Region Hallands arbete med att motverka välfärdsbrottslighet. Detta avses genomföras under våren 2026. I samband med detta planeras processarbetet övergå från att vara en avgränsad process med fokus på regionstyrelsens förvaltning till att omfatta hela Region Halland. Arbete utifrån angiven metod och mål har genomförts under året, varför riskområdets kontrollmoment anses uppfyllt. Arbete fortgår under 2026 utifrån beslutade målsättningar i regionstyrelsens verksamhetsplan, med utgångspunkt i angiven riktning i Mål- och budget 2026.

2.3 Risk för informationsläckage (IT system)

Kontrollmoment	Resultat av genomförd kontroll
Risken består i att användare inte har tillräckliga kunskaper att förstå hur de ska undvika att känslig data hamnar i orätta händer. Allt eftersom platsoberoende arbetssätt ökar och mjukvara som tjänst oftare används så ökar kraven på medarbetare, förtroendevalda och chefer att ta ansvar för att skydda regionens information. ***Beskrivning av metod:*** *Bedömning enligt SOA - en gång per år*	**Kontrollen är genomförd** Mätningar och uppföljningar som genomfördes under 2025 visar tydligt att arbetet med att stärka förmågan att skydda känslig och verksamhetskritisk information behöver fortsätta under 2026. Utöver planerade fortsatta utbildningsinsatser närmare medarbetaren startar regionen därför ett utvecklingsprojekt för att införa verktyg och processer som gör det enkelt för alla användare att klassa och skydda information i sitt dagliga arbete. I takt med att platsoberoende arbetssätt och användning av mjukvara som tjänst blir allt vanligare ställs högre krav på att medarbetare, förtroendevalda och chefer har tillräckliga kunskaper för att undvika att känslig information hanteras felaktigt eller riskerar att röjas. Nanolearning-utbildningen har under året erbjudits samtliga användare med regionadress och utgjort ett centralt verktyg för att stärka informationssäkerhetskompetensen. Utbildningen består av korta, regelbundna digitala lektioner som stödjer ett kontinuerligt lärande. Fram till augusti hade 32 % genomfört alla lektioner och ytterligare 39 % mer än hälften, medan 29 % ännu inte påbörjat utbildningen. Under hösten har utbildningen fortsatt med stabil genomförandegrad och fått mycket positiv återkoppling från flera verksamheter, som lyfter att formatet är lättillgängligt, konkret och direkt användbart i vardagen. För att praktiskt pröva förmågan att identifiera informationssäkerhetsrisker har tre fejkade phishingtester genomförts under året: • **11 april:** 18 % (2 020 användare) klickade på länken. • **4 september:** 7 % (840 användare) klickade, vilket var en tydlig förbättring jämfört med april. Cirka 400 personer fyllde i ett falskt inloggningsformulär, vilket är alarmerande. • **10 december:** 20 % (2 229 av 10 988 användare) klickade på länken. Av dessa fyllde 37 % (815 personer!) i det falska inloggningsformuläret, medan 50 % (1 108 personer) slutförde det utbildningsstöd som kopplats till testet. Årets resultat visar att förmågan att upptäcka phishing varierar över tid och att kontinuerliga utbildningsinsatser och praktiska tester fortfarande är nödvändiga. Samtidigt syns förbättrade beteenden och ökat engagemang i flera delar av organisationen. Inför 2026 genomförs en förstärkt satsning med tydligare information till förvaltningarna och förbättrad statistik på förvaltningsnivå. Syftet är att ge ökad insyn i utbildningsläget, stärka det lokala ansvarstagandet och höja deltagandegraden ytterligare. Sammantaget bedöms dessa åtgärder — i kombination med det nya projektet för att förenkla klassning och skydd av information — vara viktiga steg för att minska risken för informationsläckage i en alltmer digital arbetsmiljö.

2.4 Risk för cyberattacker (IT-system)

Kontrollmoment	Resultat av genomförd kontroll
Att kontinuitetsplaner existerar-Övande av kontinuitetsplaner - att system, speciellt sådana som är exponerade mot Internet uppdaterade. ***Beskrivning av metod*** *Manuell uppföljning* *Automatiserad sårbarhetsanalys*	**Kontrollen är genomförd** Under 2025 har Region Halland fortsatt att stärka sin förmåga till kontinuitet och robusthet inom IT-drift och informationssäkerhet. Fokus har legat på att etablera strukturerade kontinuitetsplaner, förbättra skyddet av nätverk och säkerställa att kritiska system hålls uppdaterade. **Kontinuitetsplaner och övning** Arbetet med att omsätta kontinuitetsplaner i praktiken påverkades under första halvåret av införandet av nytt journalsystem, vilket medförde att planerade övningar sköts fram. Under året har dock en **kontinuitetsplan för infrastrukturen** färdigställts, vilket etablerar en tydlig grund för hantering av större IT-störningar. Genomförande av övningar är planerade och kommer att genomföras under 2026, och kontinuitetsplanering kommer framöver att ingå som ett mål i det löpande informationssäkerhetsarbetet. **Säkerhetskopiering och återställningsförmåga** Under 2025 har arbetet med att säkra backupmiljön stärkts avsevärt. • **Säkra backuper** har etablerats. • **Regelbundna tester av återläsningar** genomförs och har visat god förmåga att återställa data. Detta innebär att regionen nu har en mer robust och verifierad återställningskapacitet vid incidenter. **Nätverkssäkerhet** Arbetet med att förbättra och skydda nätverksmiljön har fortsatt enligt plan: • Det **trådbundna nätet** har förstärkts och har nu en etablerad basnivå av säkerhet. • Motsvarande **förfining av det trådlösa nätverket** pågår och fortsätter in i 2026. Dessa åtgärder bidrar till ökad motståndskraft och minskad exponering för angrepp. **Systemkartläggning och uppdateringar** En omfattande kartläggning av system har genomförts inom flera områden, särskilt inom försörjningsflöden. Detta arbete har förbättrat överblicken över kritiska beroenden och underlag för riskstyrning. När det gäller systemuppdateringar har arbetet fortsatt, i synnerhet för de system som är exponerade mot internet. Rutiner och genomförande stärks successivt, och fler system än tidigare hålls nu uppdaterade enligt plan. **Kommande arbete** Flera prioriterade insatser fortsätter under 2026: • **Etablering av katastrofåterställningssajt (DR-site).** • **Tiering av Active Directory**, inklusive gruppering och uppdelning av administratörskonton för att höja säkerhetsnivån.

Kontrollmoment	Resultat av genomförd kontroll
	• Vidareutveckling av övningar och mognad inom kontinuitetshantering i verksamheten. **Samlad bedömning 2025** Regionen har under året etablerat en stabil grund för kontinuitetsarbete, stärkt backupförmågan och förbättrat nätverkssäkerheten. Samtidigt kvarstår behov av vidare övning och ytterligare förstärkningar inom AD-säkerhet och katastrofåterställning. Kontrollmomentet bedöms därmed som **på god väg**, men med tydliga aktiviteter som fortsätter in i 2026.

2.5 Risk med att bryta mot lagen om offentlig upphandling

Kontrollmoment	Resultat av genomförd kontroll
Stickprov på genomförda och dokumenterade direktupphandlingar. ***Beskrivning av metod:*** *Stickprov på genomförda och dokumenterade direktupphandlingar* *(urval: gärna hälften från direktupphandlingsverktyget och hälften dokumenterade på annat vis).* *a)"För att få behörighet att göra direktupphandlingar ska du: Vara utsedd av din chef och Genomfört utbildningen "Direktupphandling - inköpsutbildning för handläggare" i kompetensportalen." Kontrollera om direktupphandlingen utförts av en handläggare för direktupphandling samt om personen fått rollen.* *b)" En direktupphandling kan genomföras om värdet på inköpet inte överstiger direktupphandlingsgränsen ". Har direktupphandlingens värde understiget direktupphandlingsgränsen? (OBS ändrad gräns under feb 2022, vilken gräns beror på när DU genomförts). Kontroll av fakturor till leverantör?* *c)"Direktupphandlingen ska konkurrensutsättas i den mån det är möjligt, antingen genom att annonsera eller genom att skicka den till flera leverantörer." Har du konkurrensutsatts? Om inte, fråga handläggaren varför, är det en legitim anledning?*	**Kontrollen är genomförd** Begränsad del av direktupphandlingar utförs i verktyg för direktupphandling. En majoritet har frågat en leverantör. Stickprovet för regionkontoret av fyra leverantörer i spannet för direktupphandling visar att en av fyra köpare genomfört utbildning för direktupphandling i Kompetensportalen. a) För regionkontoret fanns 2025 totalt 181 leverantörer med spend mellan 100 000 kr – 700 000 kr (direktupphandlingar kan göras upp till 700 000 kr, undantag för bilaga 2 tjänster där beloppsgränsen är högre). Av fyra stickprov som valts av de 181 leverantörerna har ingen av upphandlingarna gjorts i verktyget för direktupphandling. För att få tillgång till verktyget behöver utbildning för direktupphandling genomföras. För ett av stickproven hade avtal tecknats. Inget av stickproven hade dokumentation enligt rutinen för direktupphandling eftersom verktyg inte används. b) Ja (utifrån faktura). c) I juni 2025 bytte Region Halland verktyg för direktupphandling. Stickprovet har genomförts på direktupphandlingar (DU) utförda i det nya verktyget, 43 st för Region Halland varav 13 st av regionkontoret. Vid nio av dessa direktupphandlingar har man fått ett anbud. I nuvarande verktyg finns inte en självklar plats för att internt dokumentera varför direktupphandlingen inte har konkurrensutsatts.