Regionernas informationssäkerhetsarbete

En uppföljning av regionernas systematiska informationssäkerhetsarbete inom hälso- och sjukvården

Sveriges Kommuner och Regioner

Innehåll

Sammanfattning

Staten och SKR har träffat överenskommelsen God och nära vård 2021. Av överenskommelsen framgår att förmågan att hantera och skydda information på ett ändamålsenligt sätt ständigt behöver utvecklas i takt med att omvärlden förändras.

Av överenskommelsen följer att regionerna ska genomföra en egen uppföljning av arbetet med informationssäkerhet, i syfte att skapa en lägesbild och identifiera eventuella utvecklingsområden.

SKR ska, tillsammans med regionerna, ta fram en gemensam struktur för regionernas uppföljning av det egna informationssäkerhetsarbetet och sammanställa resultatet av uppföljningarna.

Denna rapport utgör en sammanställning av den uppföljning av regionernas arbete med informationssäkerhet som har genomförts i enlighet med överenskommelsen.

Samordning av informationssäkerhetsarbetet

Rollen som samordnare av informationssäkerhetsarbetet är en viktig funktion för att regionen ska lyckas med sitt systematiska och riskbaserade informationssäkerhetsarbete. Av uppföljningen framgår att rollen finns utpekad i 19 av 21 regioner.

Det framgår även att den disponibla arbetstid som rollen med ansvar för att samordna informationssäkerhetsarbetet arbetar med informationssäkerhet har ökat i jämförelse med tidigare mätningar.

Ledning av informationssäkerhetsarbetet

Att uppnå och upprätthålla ett väl fungerande systematiskt och riskbaserat informationssäkerhetsarbete förutsätter en engagerad ledning och ett tydligt ledarskap på alla nivåer inom regionen.

För att ett tydligt ledarskap ska kunna realiseras förutsätts att ledningen får regelbunden avrapportering gällande den aktuella lägesbilden såsom inträffade incidenter och hantering av dessa, väsentliga förändringar i riskbilden, förslag

till förbättringar av styrande information samt förslag på justering av informationssäkerhetsarbetets inriktning och finansiering framåt.

Det har skett en tydlig förbättring sedan MSB:s rapport från 2018 sett till att regiondirektörens ledningsgrupp, i samtliga regioner, erhåller minst en föredragning årligen av informationssäkerhetsläget i den egna organisationen.

Policy, styrdokument och omfattning

Andelen regioner med politiskt antagen informationssäkerhetspolicy har ökat marginellt sedan 2018. När det gäller informationssäkerhetspolicy kan det konstateras att en markant förändring skett gällande dokumentets ålder, vilket minskat avsevärt.

Det är önskvärt och nödvändigt att den positiva trenden när det gäller uppdaterade policy även slår igenom när det gäller underliggande styrande information (exempelvis riktlinjer).

Efterlevnad

Tyngdpunkten i det uppföljande arbetet ligger på verksamheten i form av egenkontroll. Detta gäller såväl uppföljning av informationssäkerhetsrisker som uppföljning av beslutade säkerhetsåtgärders effekter.

I uppföljningen kan det konstateras en viss obalans mellan att utvärdera risker kontra att utvärdera säkerhetsåtgärders effektivitet. Här ligger utvärdering av säkerhetsåtgärders effektivitet på en lägre nivå vilket behöver ökas, inte minst för att kunna beskriva säkerhetsåtgärder i termer av erhållen verksamhetsnytta.

I uppföljningen kan konstateras att elva regioner har ett internrevisionsprogram där informationssäkerhet ingår medan nio regioner saknar detta, internrevision lyfts fram inom ISO 27001 som en viktig funktion för att ge såväl input till ledningen som att ge signal om förbättringsbehov.

Metoder

Samtliga regioner nyttjar ramverk eller standarder i sitt informationssäkerhetsarbete. Det framgår av uppföljningen att samtliga regioner använder sig av t.ex. ISO 27001. Att regionerna använder sig av standarder/ramverk ger goda förutsättningar för ett bra och tydligt samarbete mellan regionerna i olika informationssäkerhetsfrågor.

En annan viktig aspekt är livscykelperspektivet. Det framgår att antalet regioner som har en förvaltningsmodell för IT-system där informationssäkerhet vägs in har ökat från nio till 19, jämfört med tidigare mätningar.

Av uppföljningen framgår det att 20 regioner har en fastställd informationssäkerhetsklassningsmodell, att jämföra med 17 i MSB:s rapport från 2018.

Riskanalyser

20 av 21 regioner har ett beslutat arbetssätt för hantering av informationssäkerhetsrisker vilket kan jämföras med 13 av 20 i MSB:s rapport från 2018.

Utbildning

17 regioner ställer krav på att samtliga medarbetare ska genomföra en grundläggande informationssäkerhetsutbildning. Merparten av regionerna uppger också att de kräver att valda yrkesgrupper därutöver ska gå kompletterade utbildningar.

För att utbildningsinsatserna ska få avsedd effekt är det viktigt att följa upp vilka medarbetare som genomgått informationssäkerhetsutbildningen. Det finns en positiv trend inom detta område jämfört med MSB:s rapport från 2018, flera regioner uppger dessutom att detta är ett fokusområde för de närmaste åren.

Upphandling och utveckling

Antalet regioner som har ett beslutat arbetssätt för att ställa informationssäkerhetskrav vid upphandlingar och systemutveckling har ökat sedan MSB:s rapport från 2018, detta är en positiv trend som förhoppningsvis kan fortsätta så att alla regioner omfattas.

Samtidigt finns en obalans mellan att ställa informationssäkerhetskrav vid upphandlingar och att granska avtalade säkerhetsåtgärder under kontraktstiden.

Utkontrakterade (outsourcade) it-tjänster, inklusive molntjänster

Det är åtta regioner som har en outsourcingstrategi och i samtliga fall är informationssäkerhet inkluderat i strategin, vilket är en ökning från tre i MSB:s rapport från 2018.

Uppföljningen visar även att fler regioner idag ställer krav på leverantörerna att rapportera inträffade IT-incidenter till regionen än i MSB:s rapport från 2018.

Det är 15 regioner som uppger att de upphandlar molntjänster som är nödvändiga för verksamhetskritiska processer, denna siffra ska jämföras med sex i MSB:s rapport från 2018. De huvudsakliga anledningarna till att regionerna använder molntjänster inom hälso- och sjukvårdsverksamheten är t.ex. kostnadsfördelar och ökad flexibilitet.

Incidenter som påverkar informationshantering

Antalet regioner som har processer för intern rapportering respektive för hantering av informationssäkerhetsincidenter har ökat från 15 av 20 i MSB:s rapport från 2018 till 20 av 21 vid denna uppföljning.

Inledning

Bakgrund

Sveriges Kommuner och Regioner (SKR) har som ambition att stötta alla sina medlemmar till att arbeta systematiskt och riskbaserat med informationssäkerhet, för att skydda individers integritet och bevara invånarnas förtroende för välfärdsleveransen.

En väsentlig del av det systematiska och riskbaserade informationssäkerhetsarbetet är utvärdering av informationssäkerhetsarbetet och dess styrning. Genom att en organisation använder sig av en strukturerad övervakning och mätning ges förutsättningar för att utvärdera i vilken grad informationssäkerheten är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder är implementerade och fungerar tillfredsställande.

Överenskommelse mellan SKR och staten

SKR och staten har träffat överenskommelsen God och nära vård 2021.[1].

Av överenskommelsen framgår att förmågan att hantera och skydda information på ett ändamålsenligt sätt behöver ständigt utvecklas i takt med att omvärlden förändras. Individer vill att uppgifter om hälsa ska finnas tillgängliga i mötet med verksamheterna och samtidigt är det viktigt att uppgifterna hanteras säkert och skyddas från obehöriga. Därför är en trygg och säker informationshantering central för att behålla och stärka tilliten till hälso- och sjukvårdens digitalisering. Ett systematiskt informationssäkerhetsarbete är inte endast centralt för att undvika incidenter och förebygga sådant som it-intrång och informationsläckage, utan även en grundförutsättning för att möjliggöra digital verksamhetsutveckling.

Insatser som regionerna ska genomföra

För att få ta del av medlen inom ramen för utvecklingsområdet ska regionerna genomföra en egen uppföljning av arbetet med informationssäkerhet, i syfte att skapa en lägesbild och identifiera eventuella utvecklingsområden.

---

[1] God och nära vård 2021 - En omställning av hälso- och sjukvården med primärvården som nav (https://www.regeringen.se/overenskommelser-och-avtal/2021/01/god-och-nara-vard-2021---en-omstallning-av-halso--och-sjukvarden-med-primarvarden-som-nav/)

Uppföljningen bör huvudsakligen utgå ifrån de rekommendationer som Myndigheten för Samhällsskydd och Beredskap (MSB) presenterade i rapporten ”En bild av landstingens informationssäkerhetsarbete 2018 – kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten”[2]. Insatserna i övrigt kan bl.a. handla om förbättrings-arbete med anledning av uppföljningen. En del i arbetet bör även vara att ta tillvara på stöd och vägledningar från berörda statliga myndigheter, t.ex. MSB och Post- och telestyrelsen samt standardiseringsorganisationerna inom Sveriges standardiseringsförbund. Regionerna ska, med koordinering från SKR, ta fram en gemensam struktur för uppföljningen.

Insatser som SKR ska genomföra

SKR ska under 2021 fortsatt utveckla det nationella stödet och samordningen för en trygg och säker informationshantering i syfte att, i takt med förändringar i omvärlden, utveckla hälso- och sjukvårdens förmåga att hantera och skydda information på ett ändamålsenligt sätt. I detta ingår dels att tillsammans med regionerna ta fram en gemensam struktur för regionernas uppföljning av det egna informationssäkerhetsarbetet, dels att sammanställa resultatet av uppföljningarna.

Om regionerna

Regionerna ansvarar för uppgifter som är gemensamma för stora geografiska områden och som ofta kräver stora ekonomiska resurser, t.ex. hälso- och sjukvården, kultur, kollektivtrafik och att stärka regionernas tillväxt och utveckling.

[2] En bild av landstingens informationssäkerhetsarbete 2018 : kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten (https://www.msb.se/sv/publikationer/en-bild-av-landstingens-informationssakerhetsarbete-2018--kartlaggning-och-analys-av-landstingens-informationssakerhetsarbete-inom-halso--och-sjukvardsverksamheten/)

Dessa uppgifter kan delas upp i tre olika kategorier:

- Obligatoriska uppgifter
    - Hälso- och sjukvård
    - Tandvård för barn och unga upp till 23 års ålder
    - Regionalt utvecklingsansvar
- Frivilliga uppgifter
    - Kultur
    - Utbildning
    - Turism
- Gemensam, obligatorisk uppgift för kommuner och regioner
    - Regional och lokal kollektivtrafik

Antalet anställda i regionerna uppgick i november 2020 till ungefär 300 000.

Så styrs kommuner och regioner

Sverige är indelat i 21 regioner och 290 kommuner. Kommuner och regioner är självstyrande och styrs av regionalt och lokalt folkvalda politiker. Självstyret är grundlagsstadgat.

Regionens politiska beslut fattas av en folkvald församling, regionfullmäktige. Regionfullmäktige utser en regionstyrelse som leder och samordnar arbetet. Dessutom finns ett antal nämnder som har till uppgift att behandla olika ärenden som ska tas upp i fullmäktige. Nämnderna ska också verkställa de beslut som fattas.

I ett av Sveriges län skiljer sig den politiska styrningen från de övriga. Gotlands län saknar region, och istället sköts dessa uppgifter av Gotlands kommun.

Sveriges regioner är:

- Region Blekinge (länsbokstav K)
- Region Dalarna (länsbokstav W)
- Region Gotland (länsbokstav I)
- Region Gävleborg (länsbokstav X)
- Region Halland (länsbokstav N)
- Region Jämtland Härjedalen (länsbokstav Z)
- Region Jönköpings län (länsbokstav F)
- Region Kalmar län (länsbokstav H)
- Region Kronoberg (länsbokstav G)
- Region Norrbotten (länsbokstav BD)
- Region Skåne (länsbokstav M)
- Region Stockholm (länsbokstav AB)
- Region Sörmland (länsbokstav D)
- Region Uppsala (länsbokstav C)
- Region Värmland (länsbokstav S)
- Region Västerbotten (länsbokstav AC)
- Region Västernorrland (länsbokstav Y)
- Region Västmanland (länsbokstav U)
- Region Örebro län (länsbokstav T)
- Region Östergötland (länsbokstav E)
- Västra Götalandsregionen (länsbokstav O)

Uppföljningens omfattning

Uppföljningen omfattar enbart regionernas systematiska informationssäkerhetsarbete inom hälso- och sjukvårdsverksamhet, med fokus på den hälso- och sjukvård som bedrivs i egen regi (inte sådan hälso- och sjukvård som utförs av den privata sektorn, på uppdrag av regionerna).

Ingångsvärde

Ett viktigt ingångsvärde i skapandet av en gemensam struktur för uppföljningen var att utgå från de rekommendationer som MSB presenterade i sin rapport från 2018. SKR har därför gjort en översyn av de frågeställningar som låg till grund för MSB:s kartläggning 2018, samt tittat på de frågeställningar som MSB använder sig av i Infosäkkollen[3].

Tillvägagångssätt

Uppföljningen baseras på ett enkätunderlag. SKR utarbetade en webbenkät, med stöd från statistiksektionen på avdelningen för ekonomi och styrning på SKR.

Inför utskicket av webbenkäten genomfördes tre (3) informations- och dialogmöten med representanter (informationssäkerhetssamordnare eller motsvarande) från regionerna.

SKR genomförde även information och dialog med regionernas IT-direktörer.

Enkäten var tillgänglig för regionerna att besvara under perioden 13 december 2021 till den 22 april 2022. Webbenkäten skickades till registrator eller motsvarande, det vill säga regionens officiella e-postadress (t.ex. info@regionen.se). Varje region fick en enkät. Enkäten var frivillig för regionerna att besvara och enkäten besvarades av samtliga (21 av 21) regioner.

[3] Infosäkkollen är ett verktyg som stödjer uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter. (https://www.msb.se/infosakkollen)

Uppföljningen ger en bild av hur regionerna själva uppfattar sitt arbete med informationssäkerhet. Det handlar med andra ord om en uppföljning baserat på självskattning, vilket kan vara värt att ha i beaktande.

Uppföljningsområdena baseras i huvudsak på MSB:s rapport från 2018 där vissa förändringar gjorts genom att vissa frågor har tagits bort och andra har tillkommit inom respektive uppföljningsområde.

Uppföljningens delområden och resultat

Nedan redovisas, förutom en kortare beskrivning av respektive uppföljningsområden, erhållna svar samt korta iakttagelser kopplat till dessa svar.

Det kan uppfattas som om en del av frågorna inte har redovisats, sett till frågornas löpnummer, men numreringen av frågorna härleder från det verktyg som SKR använt sig av för webbenkäten. Däri ges också rubrikerna en siffra, vilket gör att det kan se ut som vissa frågor hoppats över. I redovisningen återfinns respektive frågenummer inom hakparentes.

Samordning av informationssäkerhetsarbetet

Beskrivning av området

Inom detta uppföljningsområde avses i första hand arbetet med att se till att ledning, verksamhetschefer och medarbetare får stöd i arbetet avseende informationssäkerheten inom verksamheten.

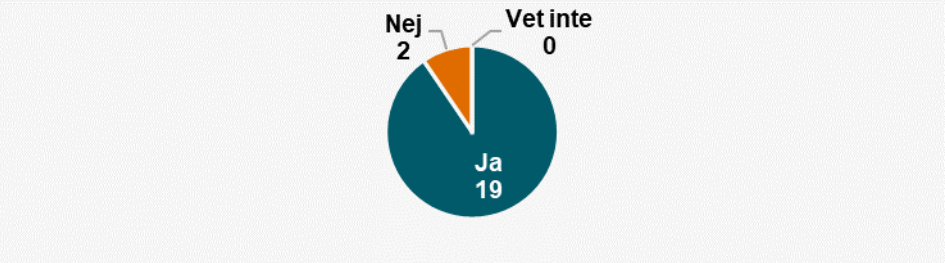
Grundprincipen är att ansvaret för själva informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret/linjen. Denna princip innebär att den person som är ansvarig för ett visst verksamhetsområde också är ansvarig för själva informationssäkerheten inom det specifika verksamhetsområdet.

Rollen informationssäkerhetssamordnare fyller en viktig funktion när det gäller samordning, rollens effektivitet är dock i sin tur beroende av:

- placering,
- mandat och
- resurstilldelning.

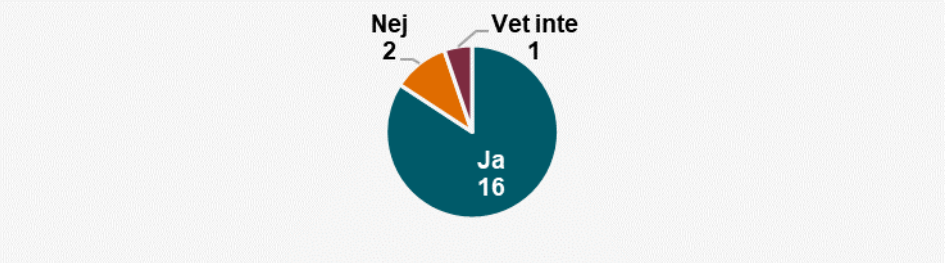
Erhållna svar

Figur 1 [4] Finns det en utpekad roll med övergripande ansvar för samordning av informationssäkerhetsarbetet inom hälso- och sjukvårdsverksamheten i regionen?



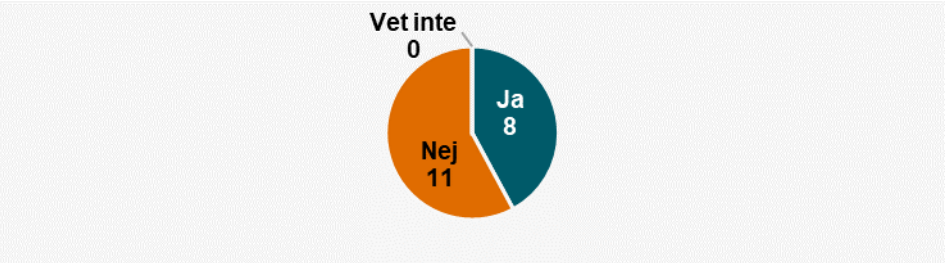
Av svaren på *fråga 4* framgår att 19 av 21 regioner har en utpekad roll för samordning av informationssäkerhetsarbetet inom hälso- och sjukvårdsverksamheten i regionen.

Figur 2 [5] Har denna roll tilldelats nödvändigt mandat som motsvarar ansvaret?



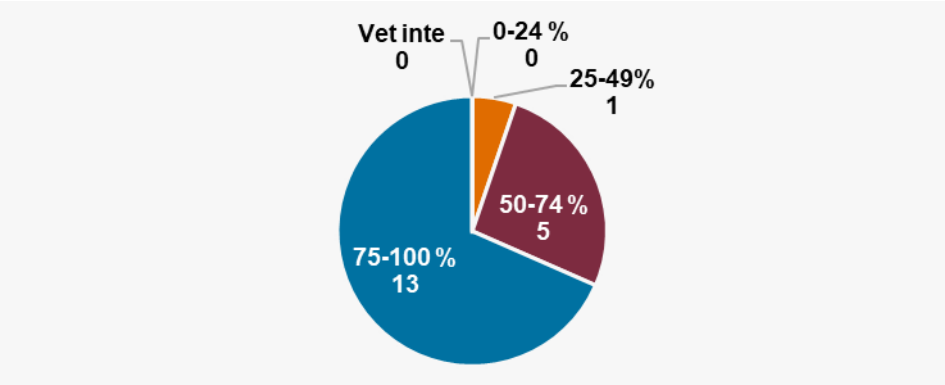
Av svaren på *fråga 5* framgår att inom 16 av de 19 regionerna anses att rollen har nödvändigt mandat.

Figur 3 [6] Disponerar rollen med övergripande ansvar för samordning av informationssäkerhet en egen budget för sitt uppdrag?



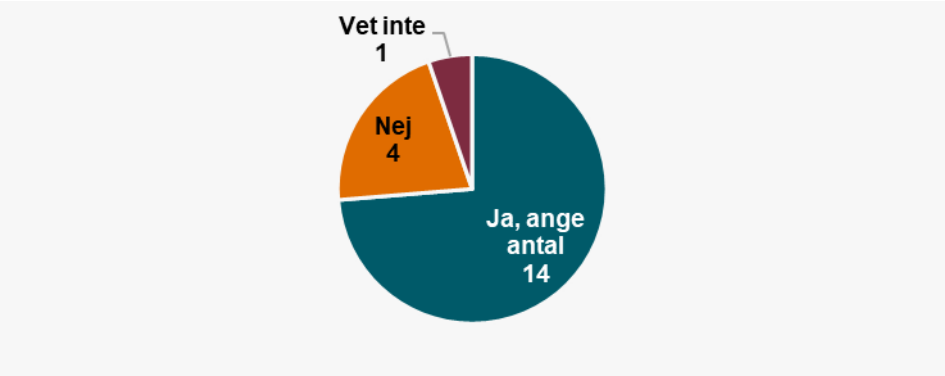
Av svaren på *fråga 6* framgår att inom åtta av de 19 regionerna har rollen en egen budget.

Figur 4 [7] Under hur stor del av arbetstiden har rollen med övergripande ansvar för samordning av informationssäkerhet möjlighet att arbeta med informationssäkerhetsfrågor?



Av svaren på *fråga 7* framgår att inom 13 av de 19 regionerna disponerar rollen 75-100% av sin arbetstid till informationssäkerhetsarbetet inom regionen.

Figur 5 [8] Finns det (utöver rollen med övergripande ansvar för samordning av informationssäkerhetsarbetet) ytterligare roller eller befattningar med uppdrag att samordna informationssäkerhetsarbetet avgränsat till viss verksamhet eller område?



Av svaren på *fråga 8* framgår att inom 14 av de 19 regionerna finns ytterligare roller eller befattningar med uppdrag att samordna informationssäkerhetsarbetet.

Figur 6 [9] Finns det andra roller eller befattningar med uppdrag att samordna informationssäkerhetsarbetet avgränsat till viss verksamhet eller område inom regionens hälso- och sjukvårdsverksamhet?

Fråga 9 besvarades endast av två regioner varför denna fråga ej tas upp närmare sett till dess begränsade uppföljningsvärde.

Iakttagelser

Rollen som samordnare av informationssäkerhetsarbetet är en viktig funktion för att regionen ska lyckas med sitt systematiska och riskbaserade informationssäkerhetsarbete. Av uppföljningen framgår att rollen finns utpekad i 19 av 21 regioner, det är två regioner som uppgett att rollen inte finns utpekad. Detta kan jämföras med MSB:s rapport från 2018 där 20 av 21 landsting/regioner uppgav att en person med utpekat ansvar för att samordna informationssäkerhetsarbetet inom landstinget/regionen fanns utpekad och att det i endast ett landsting/region saknades en utpekad person.

I 16 av de 19 regionerna som har en utpekad person anser denne att den tilldelats tillräckligt mandat som motsvarar ansvaret som följer med samordnaruppdraget.

Det är endast i åtta av de 19 regionerna som rollen för att samordna informationssäkerhetsarbetet har en egen budget, huruvida en egen budget är nödvändig eller ej framgår ej av denna uppföljning.

Vidare kan konstateras att den disponibla arbetstid som rollen med ansvar för att samordna informationssäkerhetsarbetet arbetar med informationssäkerhet har ökat, jämfört med MSB:s rapport från 2018 (siffror i parentes):

1. Det är 13 regioner (elva) som uppger att de arbetar 75-100 % med informationssäkerhet.
2. Det är fem regioner (två) som uppger att de arbetar 50-74 % med informationssäkerhet.
3. Det är en region (noll) som uppger att de arbetar 25-49 % med informationssäkerhet (*detta alternativ fanns inte i MSB:s kartläggning*).
4. Det är ingen region (sex) som uppger att de arbetar 0-24 % med informationssäkerhet.

Det framgår också av denna uppföljning att antalet regioner där det finns ytterligare roller eller befattningar med uppdrag att samordna informationssäkerhetsarbetet har ökat, från elva till 14. Det är fortsatt väldigt stor spridning på antalet definierade roller mellan regionerna, med ett spann på mellan en och 150 st.

Ledning av informationssäkerhetsarbetet

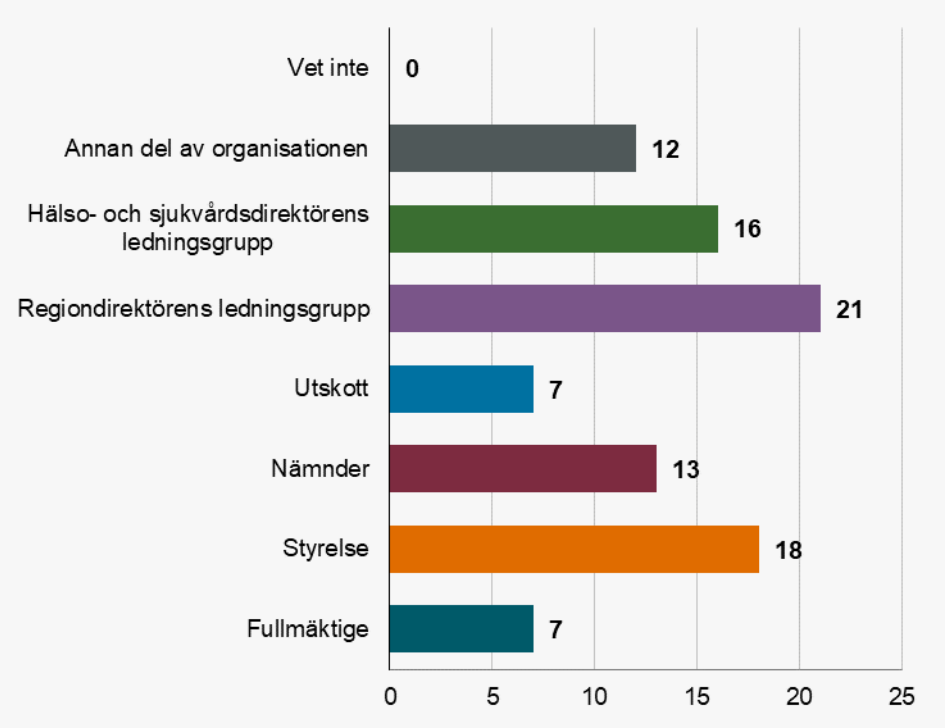
Beskrivning av området

Inom detta uppföljningsområde avses i första hand arbetet med att ge beslutsfattare underlag för att fatta beslut avseende informationssäkerheten i verksamheten. En viktig aspekt är att informationssäkerhetsarbetet och frågor kopplat till detta synliggörs och diskuteras vid möten, inte minst då detta signalerar ett tydligt ledarskap.

En annan viktig aspekt är att kartlägga om det finns brister eller ofullständigheter sett till olika typer av beslutsforum kopplat till informationssäkerhetsarbetet. En situation där endast vissa av de beslutsfattande delarna inom organisationen hanterar informationssäkerhet skulle kunna vara en signal om att ledningen behöver förbättras.

Erhållna svar

Figur 7 [11] Inom vilka delar av organisationen är informationssäkerhet på agendan?



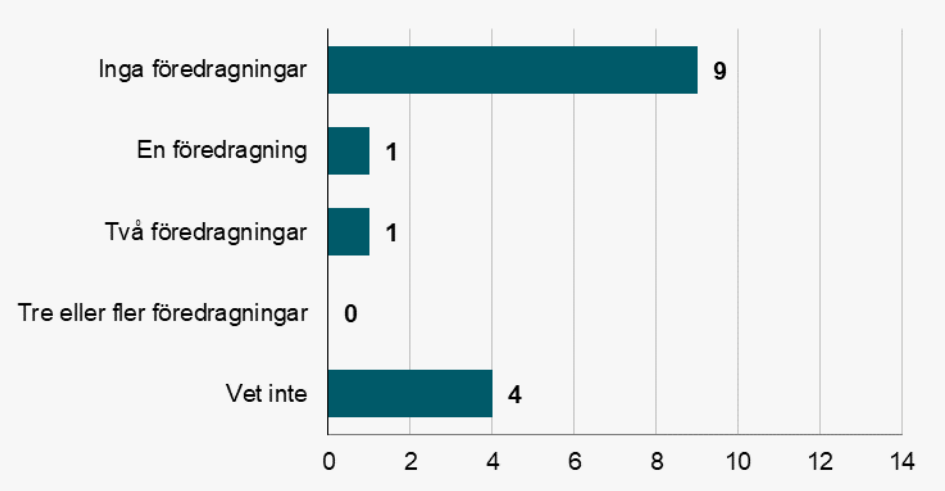
Av svaren på *fråga 11* framgår att hos samtliga svarande regioner finns informationssäkerhet på agendan hos regiondirektörens ledningsgrupp, hos en klar majoritet finns informationssäkerhet även på agendan hos styrelse respektive hos hälso- och sjukvårdsdirektörens ledningsgrupp.

Gällande om informationssäkerhet finns på agendan hos utskott respektive hos fullmäktige är andelen betydligt lägre (sju regioner).

Under kategorin ”annan del av organisationen” som besvarats av tolv regioner anges även en god spridning av olika mer förvaltningsnära funktioner inom organisationen.

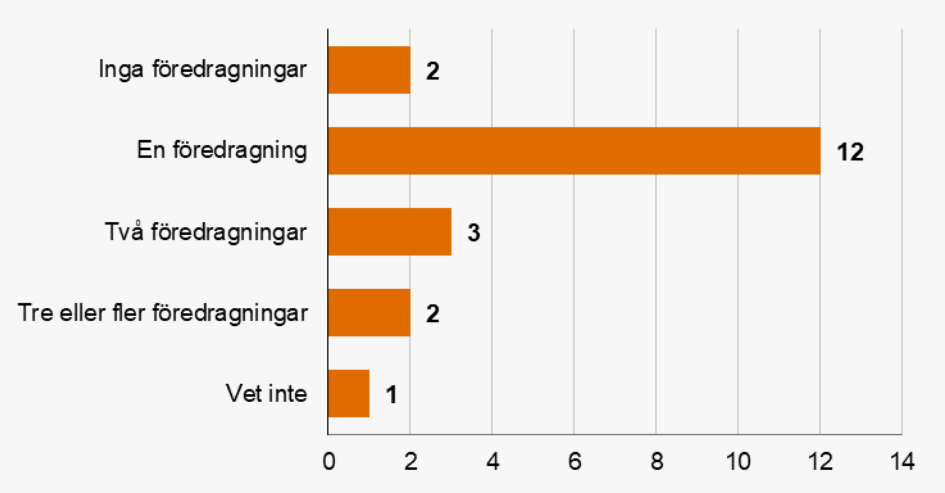
Frågorna 12.1-12.7 har besvarats av upp till 20 regioner.

Figur 8 [12.1] Hur många föredragningar kopplade till informationssäkerhet görs vanligen under ett år i de olika delarna av organisationen? ***Fullmäktige***



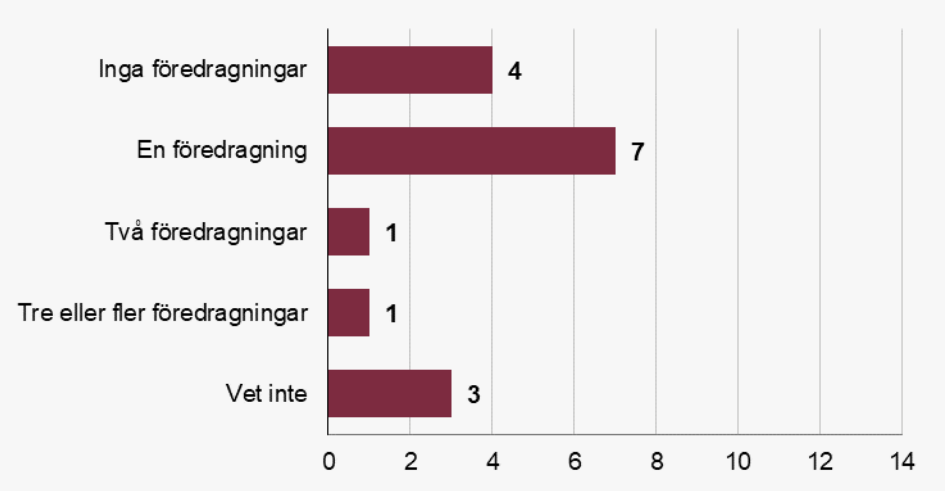
Av svaren på *fråga 12.1* framgår att endast två av 15 regionfullmäktige fått föredragning kopplade till informationssäkerhet.

Figur 9 [12.2] Hur många föredragningar kopplade till informationssäkerhet görs vanligen under ett år i de olika delarna av organisationen? ***Styrelse***



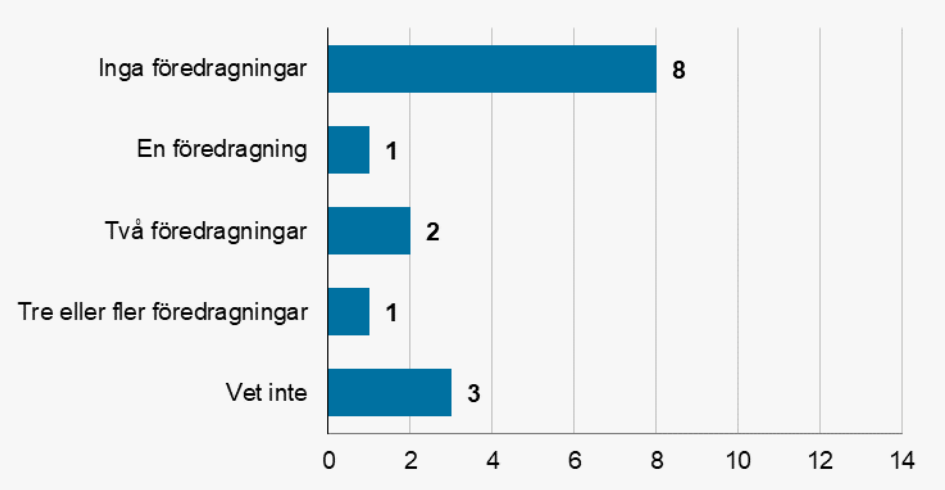
Av svaren på *fråga 12.2* framgår att 17 av 20 regionstyrelser får en eller flera föredragningar kopplade till informationssäkerhet. I två av regionerna ges inga föredragningar till regionstyrelsen.

Figur 10 [12.3] Hur många föredragningar kopplade till informationssäkerhet görs vanligen under ett år i de olika delarna av organisationen? ***Nämnder***



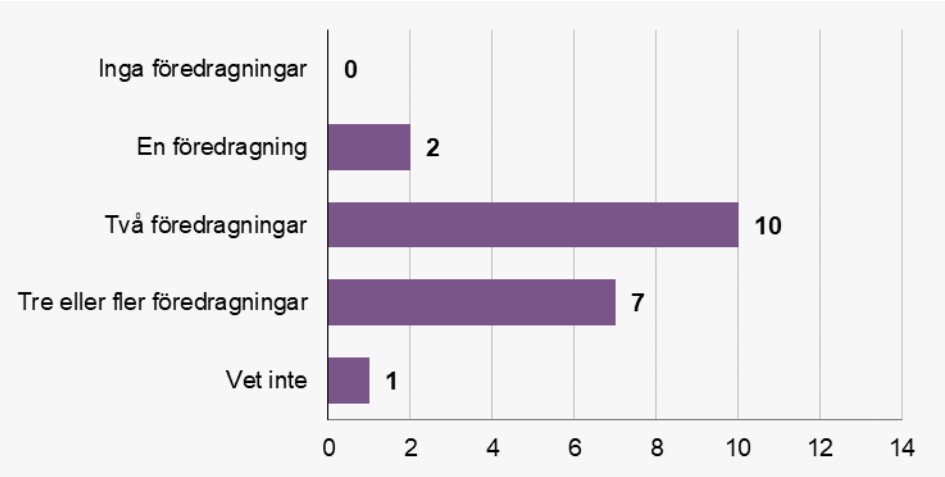
Av svaren på *fråga 12.3* framgår att i nio av 16 regioner får olika nämnder en eller flera föredragningar kopplade till informationssäkerhet. I fyra av regionerna ges inga föredragningar till nämnder.

Figur 11 [12.4] Hur många föredragningar kopplade till informationssäkerhet görs vanligen under ett år i de olika delarna av organisationen? ***Utskott***



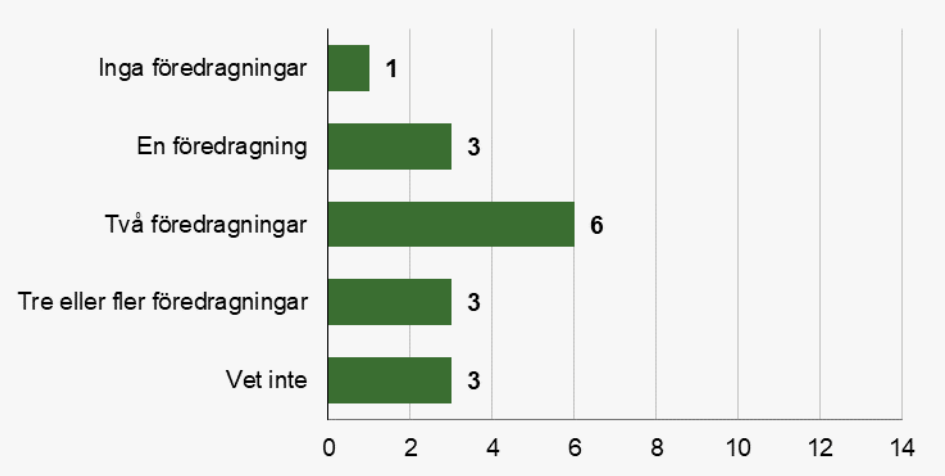
Av svaren på *fråga 12.4* framgår att i fyra av 15 regioner får olika utskott en eller flera föredragningar kopplade till informationssäkerhet. I åtta av regionerna ges inga föredragningar till utskott.

Figur 12 [12.5] Hur många föredragningar kopplade till informationssäkerhet görs vanligen under ett år i de olika delarna av organisationen? ***Regiondirektörens ledningsgrupp***



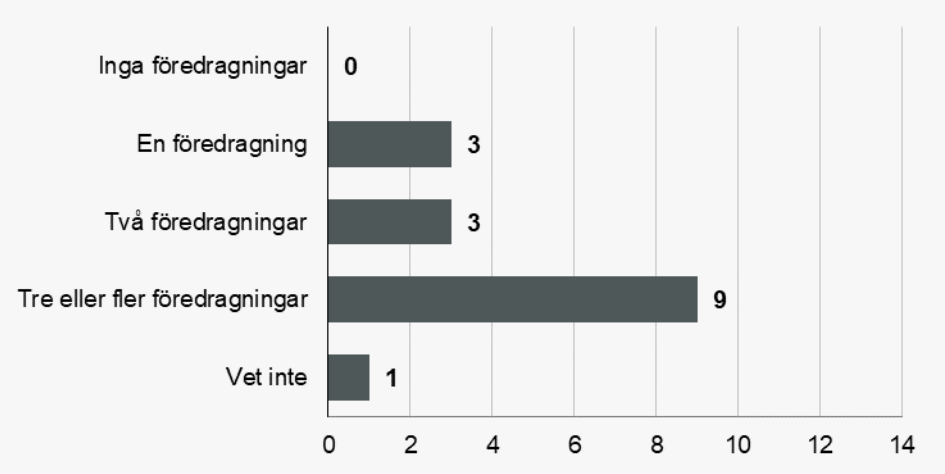
Av svaren på *fråga 12.5* framgår att i 19 av 20 regioner får Regiondirektörens ledningsgrupp en eller flera föredragningar kopplade till informationssäkerhet.

Figur 13 [12.6] Hur många föredragningar kopplade till informationssäkerhet görs vanligen under ett år i de olika delarna av organisationen? ***Hälso- och sjukvårdsdirektörens ledningsgrupp***



Av svaren på *fråga 12.6* framgår att i tolv av 16 regioner får Hälso- och sjukvårdsdirektörens ledningsgrupp en eller flera föredragningar kopplade till informationssäkerhet. I en av regionerna ges ingen föredragning för Hälso- och sjukvårdsdirektörens ledningsgrupp.

Figur 14 [12.7] Hur många föredragningar kopplade till informationssäkerhet görs vanligen under ett år i de olika delarna av organisationen? ***Annan del av organisationen***



Av svaren på *fråga 12.7* framgår att i 15 av 16 regioner får andra delar av organisationen en eller flera föredragningar kopplade till informationssäkerhet.

Iakttagelser

Det har skett en tydlig förbättring sedan MSB:s rapport från 2018 sett till att regiondirektörens ledningsgrupp erhåller minst en föredragning hos samtliga svarande regioner (med reservation för svaret ”vet ej”).

Det är även en förbättring då antalet regioner som svarar två föredragningar har ökat från fem till tio.

Den organisationsdel som erhåller minst antal föredragningar per år är fullmäktige där 1 region svarar ”två föredragningar”, 1 region svarar ”en föredragning” och nio regioner svarar ”inga föredragningar”.

Policy, styrdokument och omfattning

Beskrivning av området

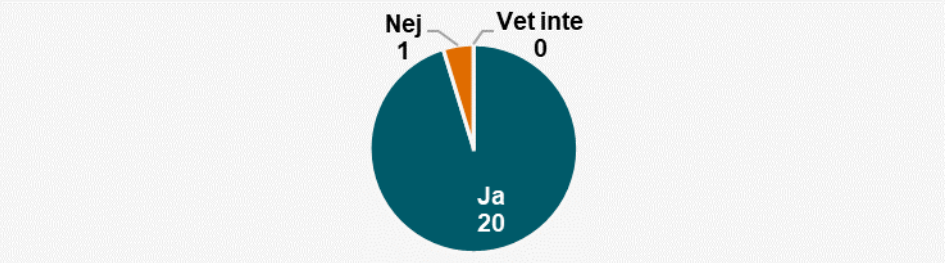
Inom detta uppföljningsområde avses i första hand arbetet med ett policydokument som lägger grunden för ett systematiskt och riskbaserat informationssäkerhetsarbete. En policy är ledningens viljeyttring vad avser informationssäkerhetens inriktning och ger det strategiska perspektivet. Policydokumentet svarar på frågor såsom vad informationssäkerhet är, vilka

risker som ska reduceras, ambitioner och mål, vem som ansvarar för vad på övergripande nivå och var det finns mer information om informations-säkerhetsarbetet.

Policyn konkretiseras genom styrande dokument som exempelvis riktlinjer, anvisningar, rutiner eller vägledningar för informationssäkerhet. Dessa dokument berättar mer i detalj vad som gäller för organisationens systematiska och riskbaserade informationssäkerhetsarbete för olika målgrupper i verksamheten.

Erhållna svar

Figur 15 [14] Finns en gällande informationssäkerhetspolicy som är politiskt antagen?



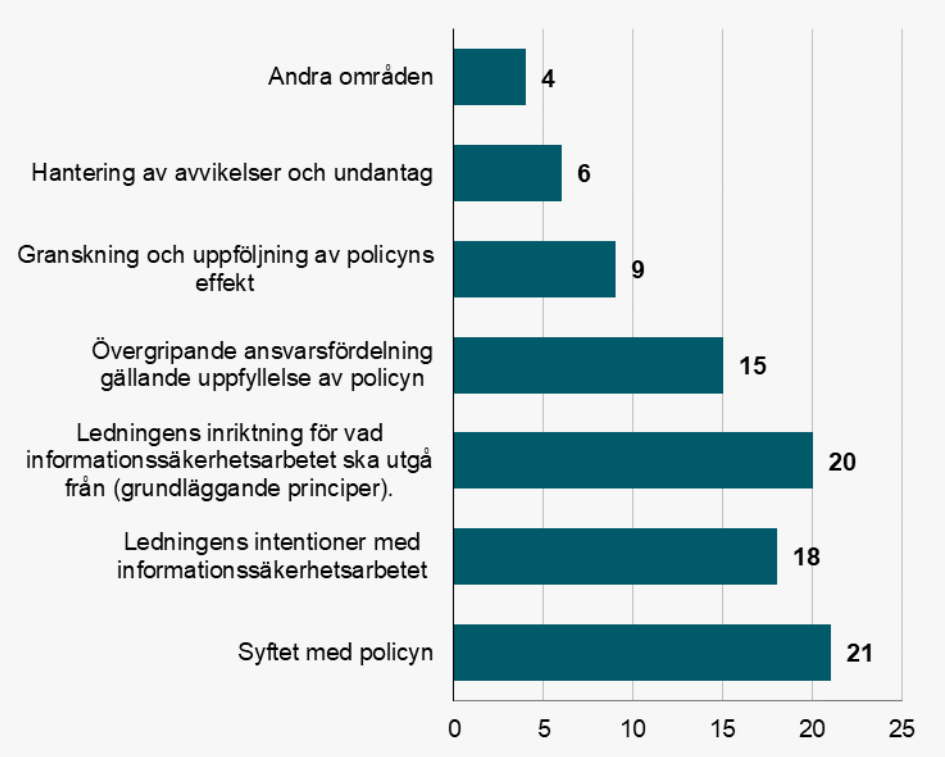
Av svaren på *fråga 14* framgår att 20 av 21 svarande regioner har en politiskt antagen gällande informationssäkerhetspolicy.

Figur 16 [15] När fastställdes/reviderades nuvarande informationssäkerhetspolicy?

Av svaren på *fråga 15* som besvarats av 20 regioner framgår att:

- Sju regioner har en policy som antagits för mindre än ett år sedan,
- Tio regioner har en policy som antagits för ett till tre år sedan, samt att
- Tre regioner har en policy som antagits för mer än tre år sedan.

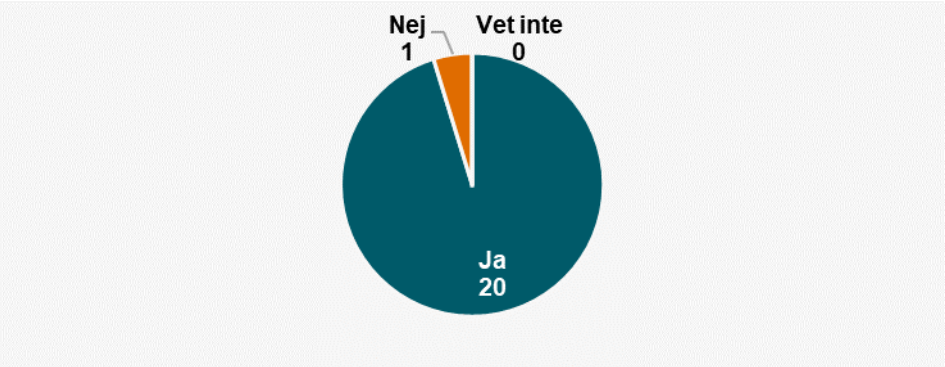
Figur 17 [16] Vilka områden definieras i informationssäkerhetspolicyn?



Av svaren på *fråga 16* som besvarats av 21 regioner framgår att:

- hos en stor majoritet av regionerna (hos 18-21 regioner) omfattar policyn beskrivning av; policyns syfte, ledningens intentioner samt ledningens inriktning,
- hos 15 av regionerna beskrivs övergripande ansvarsfördelning,
- det kan noteras att områden så som; granskning och uppföljning av policyns effekt, hantering av avvikelser och undantag samt mål och avgränsningar tas upp hos betydligt färre regioner (upp till nio regioner).

Figur 18 [17] Inkluderas regionens medicinska informationssystem i det samordnade informationssäkerhetsarbetet?



Av svaren på *fråga 17* som besvarats av samtliga regioner framgår att hos 20 av regionerna inkluderas de medicinska IT-systemen i det samordnade informationssäkerhetsarbetet.

Iakttagelser

Andelen svarande med politisk antagen informationssäkerhetspolicy har ökat marginellt sedan 2018.

När det gäller informationssäkerhetspolicy kan det konstateras att en markant förändring skett gällande dokumentets ålder, vilket minskat avsevärt. Den identifierade förskjutningen mot ”nyare” policys är en indikation på anpassningar till förändrade behov och hänsynstaganden gällande vad som ska uppnås.

Informationssäkerhetspolicyn hos i princip alla svarande regioner uttrycker; syfte med policyn, ledningens intentioner respektive inriktning gällande informationssäkerhetsarbetet samt övergripande ansvarsfördelning.

Det är önskvärt och nödvändigt att den positiva trenden när det gäller uppdaterade policy även slår igenom när det gäller underliggande styrande information (exempelvis riktlinjer). Detta så att den styrande informationen anpassas till och konkretiserar en uppdaterad informationssäkerhetspolicy.

Efterlevnad

Beskrivning av området

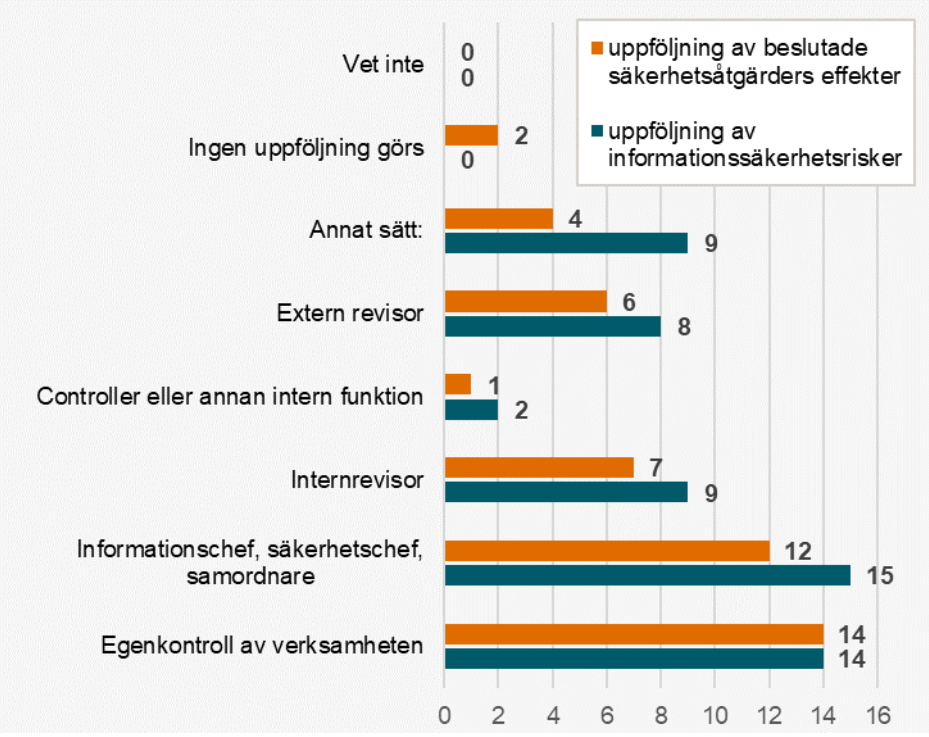
Inom detta uppföljningsområde avses i första hand hur informationssäkerhetsarbetet efterlevs.

En grundförutsättning för att kunna bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete är att löpande följa upp och utvärdera arbetet i syfte att förbättra och anpassa arbetet utifrån organisationens behov.

De åtgärder som införs i organisationen, tekniska såväl som administrativa, behöver kunna följas upp och utvärderas för att säkerställa att de möter de risker och möjligheter som identifierats. En central del av ledningens uppföljning och utvärdering utgörs sedan av att rollen som samordnare för det systematiska och riskbaserade informationssäkerhetsarbetet får avrapportera resultaten för ledningen om hur arbetet med informationssäkerhet fortlöper.

Erhållna svar

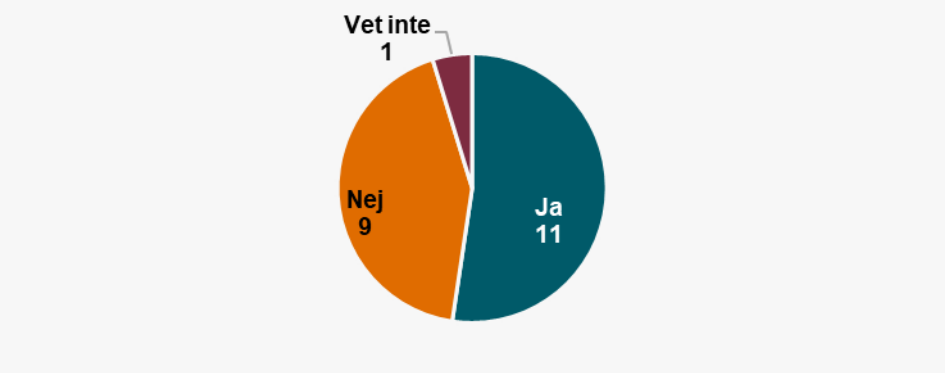
Figur 19 [19] Vem eller vilka genomför uppföljning av informationssäkerhetsrisker? [20] Vem eller vilka genomför uppföljning av beslutade säkerhetsåtgärders effekter?



Av svaren på *fråga 19*, framgår att hos samtliga regioner (21 av 21) genomförs uppföljning. Majoriteten anger att det utförs av verksamheten genom egenkontroll respektive av informationssäkerhetschef motsv. Även andra roller anges fast då med en något lägre representation.

Av svaren på *fråga 20*, framgår att hos 19 av 21 svarade regioner genomförs uppföljning. På liknande sätt som vid fråga 19 anger majoriteten att uppföljning görs av verksamheten genom egenkontroll. En något lägre andel anger uppföljning via informationssäkerhetschef motsv. Övriga roller har en klart lägre representation vid fråga 20 jämfört med fråga 19.

Figur 20 [21] Finns det ett internrevisionsprogram gällande informationssäkerhet?



Av svaren på fråga 21 framgår att elva av regionerna har ett internrevisionsprogram gällande informationssäkerhet, däremot svarar nio regioner att ett internrevisionsprogram gällande informationssäkerhet saknas.

Av svaren på fråga 22[4] framgår att de elva regionernas internrevisionsprogram gällande informationssäkerhetens omfattning varierar, några exempel:

- Alla förvaltningar
- Hälso- och sjukvårdens alla förvaltningar
- Kopplat till certifieringens omfattning.
- 2022 är det främst förvaltning för digitaliseringen.
- Internrevisorerna gör en årlig plan där inriktningen varierar mellan åren. Samtliga verksamheter omfattas av internrevisionsprogrammet.

[4] [22] Beskriv vilka delar av verksamheten som omfattas av internrevisionsprogrammet

Iakttagelser

Tyngdpunkten i det uppföljande arbetet ligger på verksamheten i form av egenkontroll. Detta gäller såväl uppföljning av informationssäkerhetsrisker som uppföljning av beslutade säkerhetsåtgärders effekter. Av uppföljningen framgår att detta sker hos 14 av 20 regioner.

Rollen som samordnare för det systematiska och riskbaserade informationssäkerhetsarbetet (informationssäkerhetschef, säkerhetschef, informationssäkerhetssamordnare eller motsv.) har på samma sätt som egenkontroller i verksamheten en central funktion när det gäller uppföljning av informationssäkerhetsrisker och säkerhetsåtgärders effekter. Av uppföljningen framgår att detta sker hos 15 av 20 regioner respektive hos tolv av 20 regioner.

För övriga namngivna roller/funktioner är bilden dock att uppföljning av säkerhetsåtgärders effekter är betydligt lägre än uppföljning av informations-säkerhetsrisker. Det kan behöva analyseras djupare då dessa två områden har en stark koppling till varandra.

Nio regioner anger att de inte har något internrevisionsprogram gällande informationssäkerhet. Med hänsyn till att internrevision lyfts fram inom ISO 27001 som en viktig funktion för att ge såväl input till ledningen som att ge signal om förbättringsbehov är detta ett förbättringsområde.

Att säkerställa efterlevnad och utvärdera progress gällande informationssäkerhet är centralt i arbetet med att uppnå ständiga förbättringar. För att gynna ett systematiskt och riskbaserat informationssäkerhetsarbete behöver det finnas roller med uttalat ansvar att utvärdera informationssäkerhetsarbetet. I denna uppföljning kan konstateras att det i regel finns ett flertal roller med detta ansvar vilket är mycket positivt.

Av uppföljningen framkommer en viss obalans mellan att utvärdera risker kontra att utvärdera säkerhetsåtgärders effektivitet. Här ligger utvärdering av säkerhetsåtgärders effektivitet på en lägre nivå vilket behöver ökas, inte minst för att kunna beskriva säkerhetsåtgärder i termer av erhållen verksamhetsnytta.

I uppföljningen kan konstateras att elva regioner har ett internrevisionsprogram där informationssäkerhet ingår medan nio regioner saknar detta. Förbättringen sedan 2018 är här endast marginell, där nio landsting/regioner saknade internrevisionsprogram.

Metoder

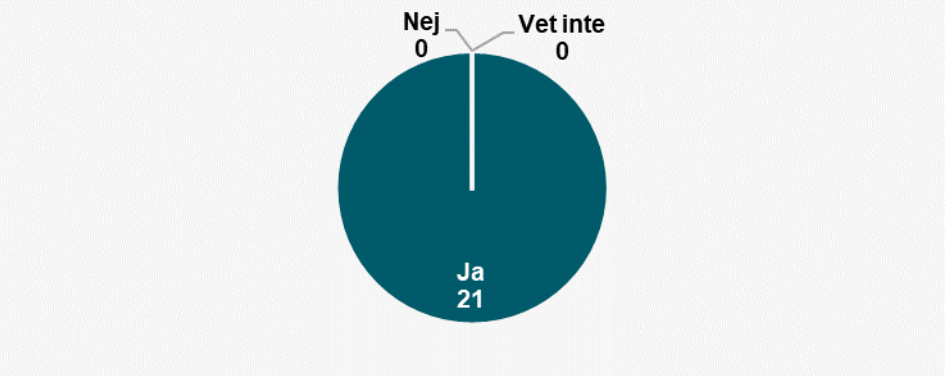
Beskrivning av området

Inom detta uppföljningsområde avses dels regionernas förhållningssätt till ramverk och standarder inom informationssäkerhetsområdet och dels förekomsten av informationsklassningsmodeller.

Genom att följa ett eller flera ramverk och standarder kan kvaliteten i det systematiska och riskbaserade informationssäkerhetsarbetet gynnas genom att man utgår från beprövade idéer och koncept. En viktig aspekt i sammanhanget är att de flesta ramverk och standarder behöver anpassas sett till den aktuella organisationen för att uppnå avsedd effekt och nytta. Informationssäkerhets-klassning tillämpas för att värdera olika tillgångar och utgör därmed en viktig grund i informationssäkerhetsarbetet.

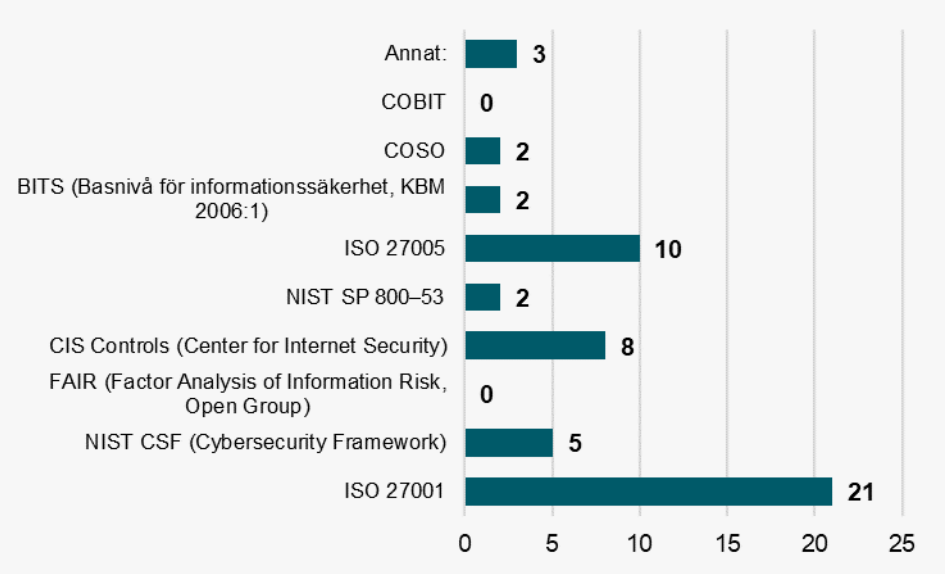
Erhållna svar

Figur 21 [24] Använder regionen någon/några ramverk eller standarder som stöd i det systematiska informationssäkerhetsarbetet?



Av svaren på *fråga 24* framgår att samtliga regioner (21 av 21) nyttjar ramverk eller standarder i sitt informationssäkerhetsarbete.

Figur 22 [25] Vilka/vilka ramverk eller standarder används som stöd för regionens systematiska informationssäkerhetsarbete?

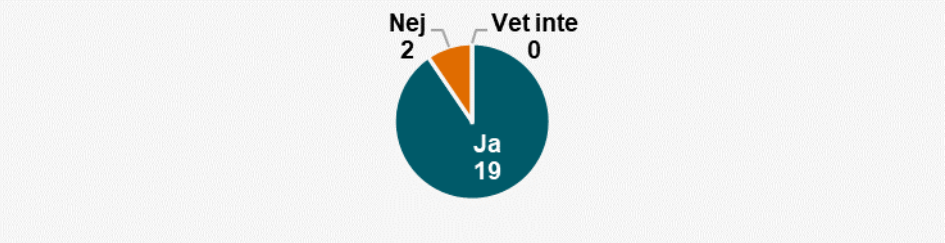


Av svaren på *fråga 25* framgår att samtliga regioner använder ISO 27001. Utöver ISO 27001 är de mest använda standarderna/ramverken:

- ISO 27005 som används av tio regioner,
- CIS Controls som används av åtta regioner och
- NIST CSF som används av fem regioner.

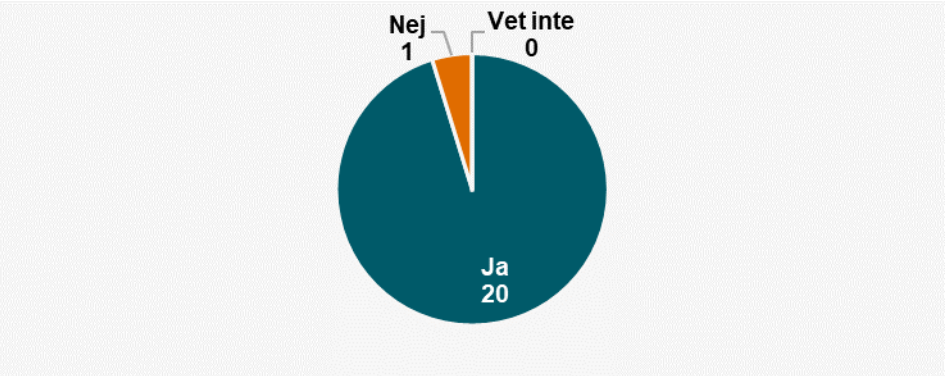
Noterbart är att 2 regioner anger att man fortfarande använder BITS som utgavs 2006 av MSB:s ”föregångare” Krisberedskapsmyndigheten (KBM).

Figur 23 [26] Finns det en förvaltningsmodell inom hälso- och sjukvårdsverksamheten för IT-system i vilken informationssäkerhet vägs in?



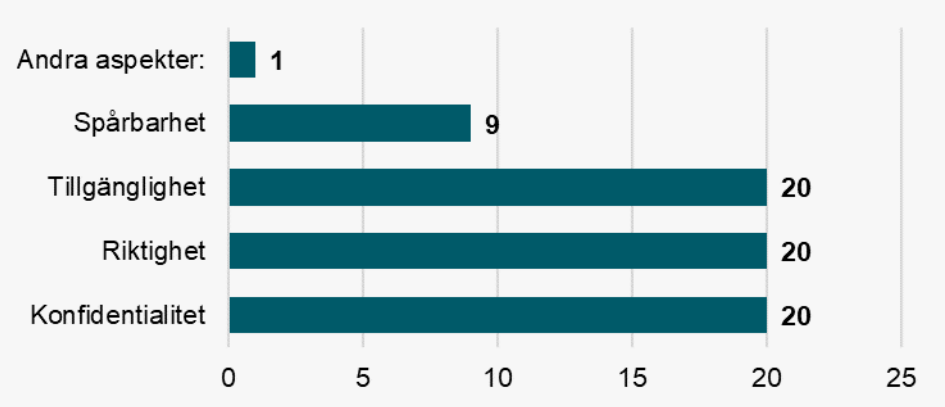
Av svaren på *fråga 26* framgår att 19 av 21 regioner har en förvaltningsmodell för IT-system där informationssäkerhet vägs in.

Figur 24 [27] Har regionen en fastställd informationsklassningsmodell?



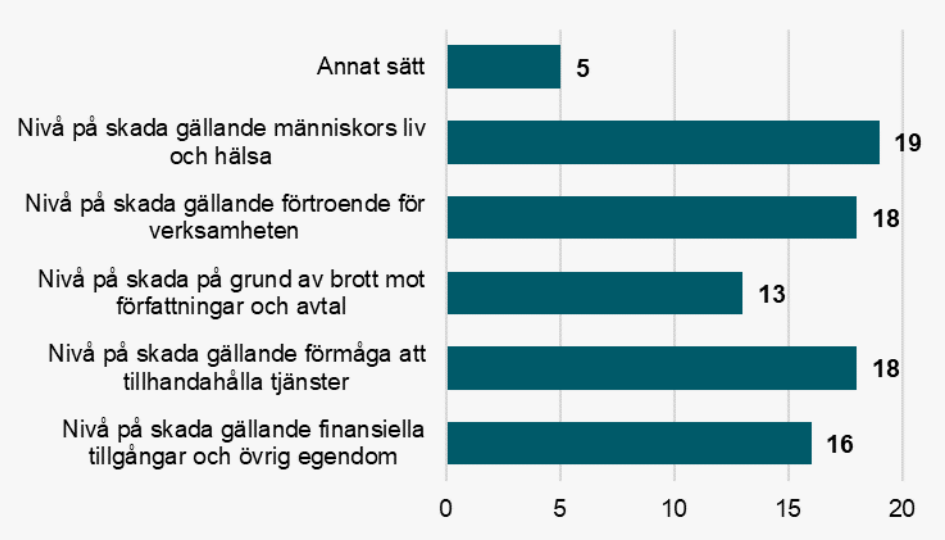
Av *fråga 27* framgår att 20 av 21 svarande regioner har en fastställd informationssäkerhetsklassningsmodell.

Figur 25 [28] Vilka aspekter omfattas av regionens informationsklassning?



Av *fråga 28* framgår att informationssäkerhetsklassningsmodellen hos samtliga av dessa 20 regioner omfattar Konfidentialitet, Riktighet samt Tillgänglighet. nio regioner svarar att modellen även omfattar Spårbarhet.

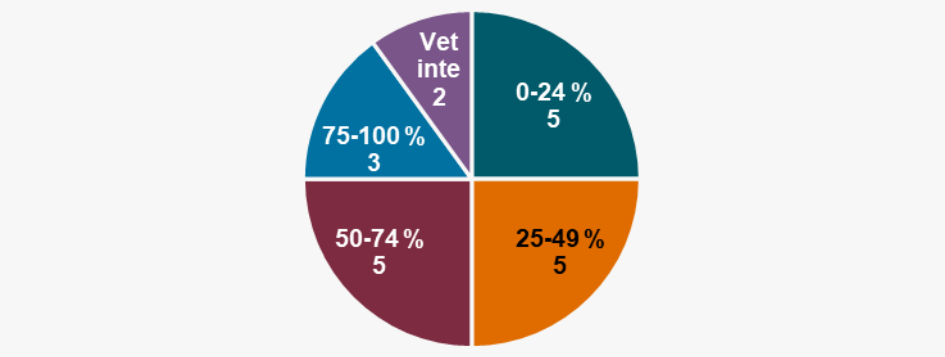
Figur 26 [29] Vad baseras informationsklassningen på?



Av *fråga 29* framgår att informationssäkerhetsklassningen i första hand baseras på:

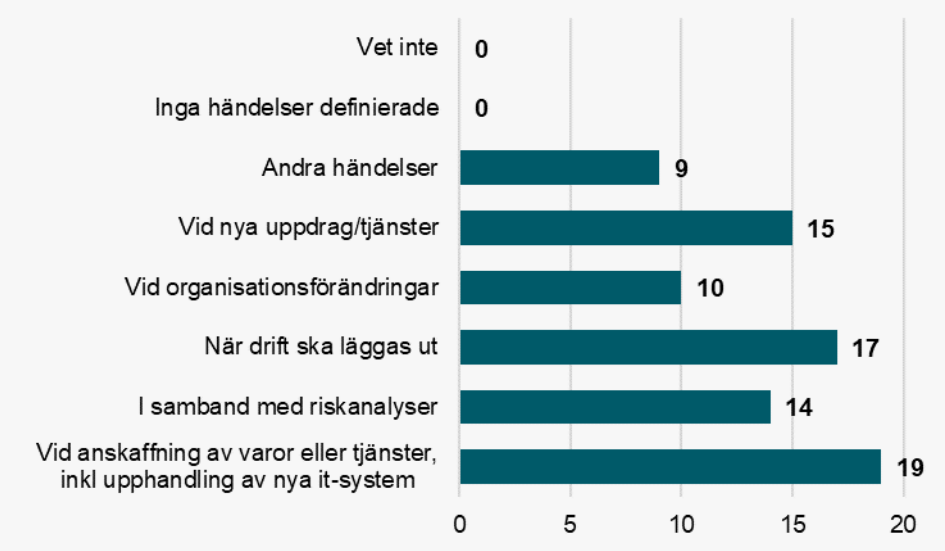
- nivå av skada på människors liv och hälsa,
- nivå av skada gällande förtroende för verksamheten och
- nivå av skada gällande förmåga att tillhandahålla tjänster.

Figur 27 [30] Hur stor andel av informationstillgångarna inom hälso- och sjukvårdsverksamheten i regionen uppskattas vara informationssäkerhetsklassade?



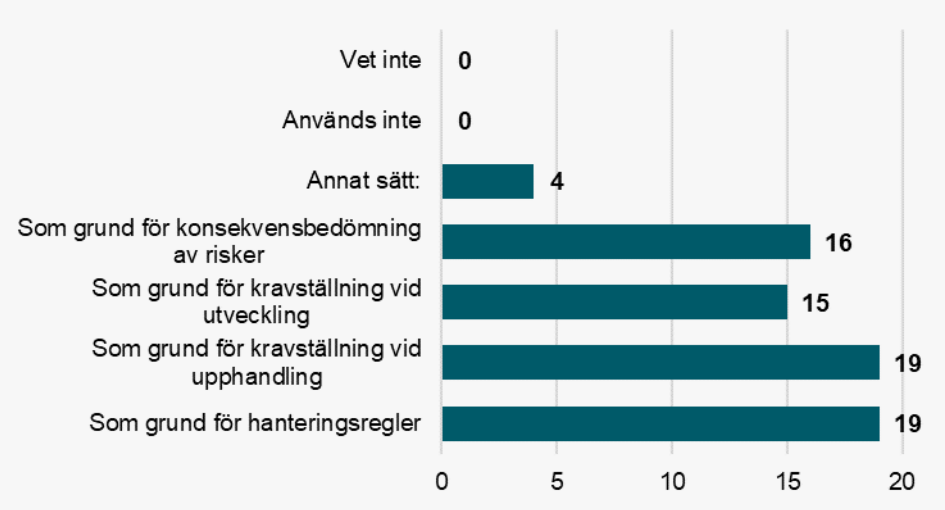
Av svaren på *fråga 30* framgår en relativt jämn spridning av hur regionerna uppskattar vilken andel av informationstillgångarna som är informationssäkerhetsklassade.

Figur 28 [31] Vid vilka händelser ska informationsklassning ske inom hälso- och sjukvårdsverksamheten?



Av svaren på *fråga 31*, där 19 regioner svarade, framgår att informationssäkerhetsklassning huvudsakligen kopplas till IT-relaterade händelser, d.v.s. vid anskaffning respektive när drift ska läggas ut. Överlag görs en tydlig koppling mellan informationssäkerhetsklassning och just förändrade omständigheter, endast en region nämner att det också görs vid årlig uppföljning.

Figur 29 [32] På vilket sätt används klassningsmodellen i informationssäkerhetsarbetet?



Av svaren på *fråga 32*, där 20 regioner svarade, framgår att 19 regioner använder informationssäkerhetsklassningsmodellen som grund för hanteringsregler respektive som grund för kravställning vid upphandling. En något lägre andel svarande använder informationssäkerhetsklassningsmodellen som grund för konsekvensbedömning av risker (16 st) respektive som grund för kravställning vid utveckling (15 st). Under ”annat sätt” samt som kommentar nämns även att informationssäkerhetsklassningsmodellen används för att få ett adekvat skydd respektive att klassningen automatiskt ger skyddsmekanismer för angiven klassningsnivå.

Iakttagelser

Samtliga regioner nyttjar ramverk eller standarder i sitt informationssäkerhetsarbete. Det framgår av uppföljningen att samtliga regioner (21 av 21) använder sig av ISO 27001.

Regionerna uppger även att de använder en del andra standarder/ramverk i sitt informationssäkerhetsarbete, dessa är bland annat ISO 27005, CIS Controls och NIST CSF.

Att regionerna använder sig av olika standarder/ramverk ger goda förutsättningar för ett bra och tydligt samarbete mellan regionerna i olika informationssäkerhetsfrågor.

Det är värt att notera att två regioner anger att man fortfarande använder BITS (Basnivå för informationssäkerhet) som utgavs 2006 av MSB:s ”föregångare” KBM.

En annan viktig aspekt i det systematiska och riskbaserade informationssäkerhetsarbetet är livscykelperspektivet. Antalet regioner som har en förvaltningsmodell för IT-system där informationssäkerhet vägs in har ökat från nio till 19 (mellan 2018 och 2022).

Av denna uppföljning framgår att det är 20 regioner som har en fastställd informationssäkerhetsklassningsmodell, att jämföra med 17 i MSB:s rapport från 2018. Hos samtliga regioner omfattar informationssäkerhetsklassnings-modellen aspekterna Konfidentialitet, Riktighet och Tillgänglighet, hos nio regioner omfattar modellen även aspekten Spårbarhet.

En av de centrala delarna i ett systematiskt och riskbaserat informations-säkerhetsarbete är att organisationens informationstillgångar ges rätt skydd,

d.v.s. alla informationstillgångar är inte i behov av samma skydd, det är därför viktigt att regionerna informationssäkerhetsklassificerar sina informationstillgångar. Det är en relativt jämn spridning mellan regionerna avsett hur stor andel av informationstillgångarna inom hälso- och sjukvårdsverksamheten som har informationssäkerhetsklassificerats. Det är positivt att se att regionerna kommit framåt i arbetet med att informationssäkerhetsklassificera sina informationstillgångar jämfört med MSB:s rapport från 2018, då hade 16 landsting/regioner informationssäkerhetsklassificerat upp till 25 % av informationstillgångarna, i denna uppföljning har 13 regioner klassat minst 25% av informationstillgångarna (varav 8 regioner klassat minst 50%).

Det finns en tydlig koppling mellan informationssäkerhetsklassning och förändrande omständigheter, t.ex. olika IT-relaterade händelser, som anskaffning och outsourcing. Informationssäkerhetsklassning används som grund för hanteringsregler respektive som grund för kravställning vid upphandling hos 19 av regionerna. Flera regioner använder också informationssäkerhetsklassningsmodellen som grund för konsekvensbedömning av risker och för kravställning vid utveckling.

Riskanalyser

Beskrivning av området

Inom detta uppföljningsområde avses i första hand riskanalyser betraktat som en central del i det systematiska och riskbaserade informationssäkerhetsarbetet.

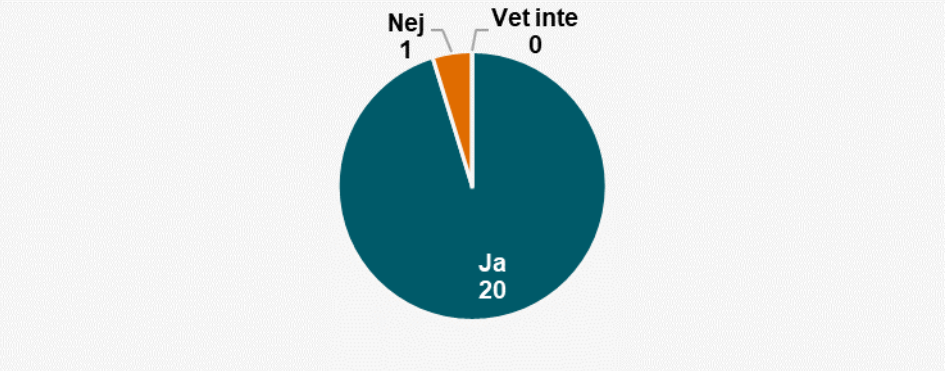
Syftet med riskanalys är att skapa ett beslutsunderlag som identifierar de väsentliga riskerna avseende informationssäkerhet. Verksamheten kan på så sätt bedöma och prioritera riskerna. Risker som inte kan accepteras behöver sedan åtgärdas på ett ändamålsenligt sätt.

För att vara effektiva ska riskanalyser ske regelbundet och/eller inför förändringar som kan tänkas påverka riskerna eller införa nya risker. Identifiering av risker behöver inkludera allt från informationsteknik, processer, till sättet att styra informationssäkerheten.

Vid riskanalyser är det centralt att säkerställa att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat.

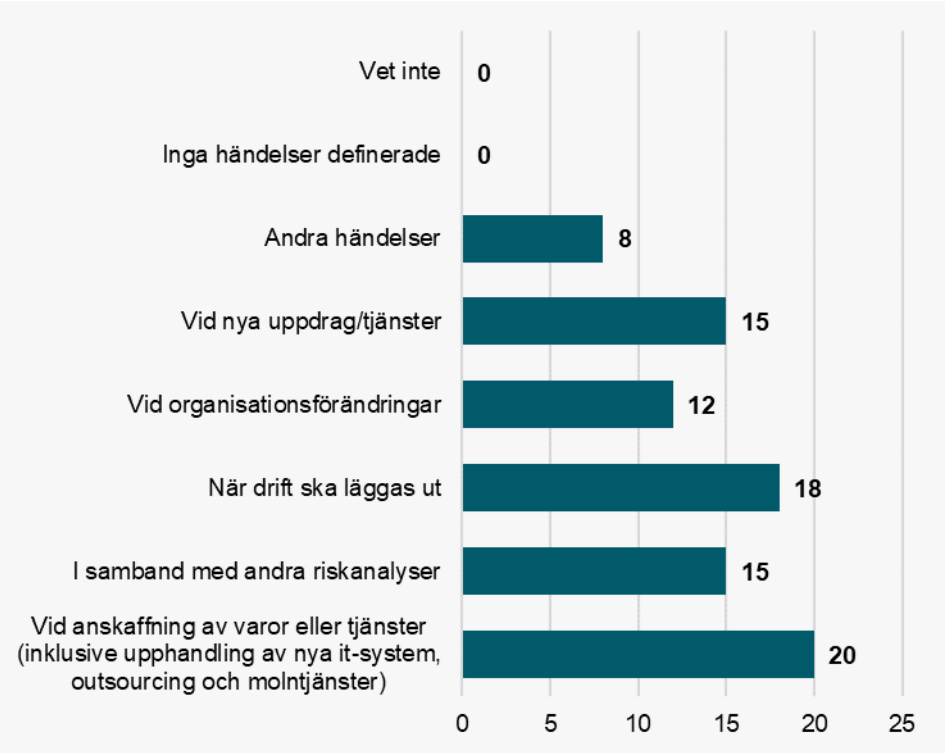
Erhållna svar

Figur 30 [34] Finns ett beslutat arbetssätt (inklusive roller och ansvarsområden) för hantering av informationssäkerhetsrisker inom regionens hälso- och sjukvårdsverksamhet?



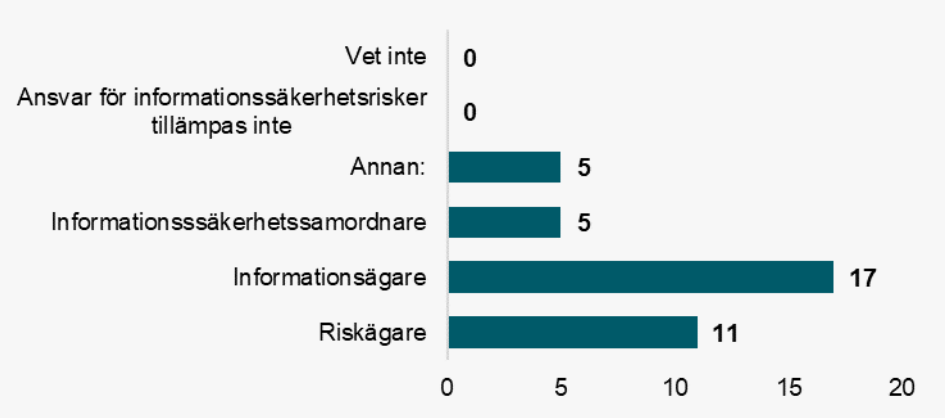
Av svaren på *fråga 34* framgår att 20 av 21 regioner har ett beslutat arbetssätt för hantering av informationssäkerhetsrisker.

Figur 31 [35] Vid vilka händelser ska riskanalyser ske avseende informationssäkerhet inom hälso- och sjukvårdsverksamheten?



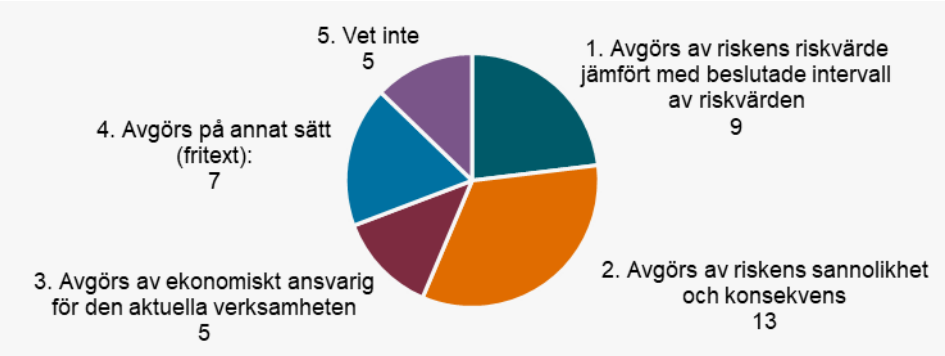
Av svaren på *fråga 35* framgår att riskanalyser gällande IT-relaterade händelser är framträdande, 20 respektive 18 svar, samtidigt som ej IT-relaterade händelser också har god representation.

Figur 32 [36] Vilka roller/befattningar ansvarar för identifierade informationssäkerhetsrisker?



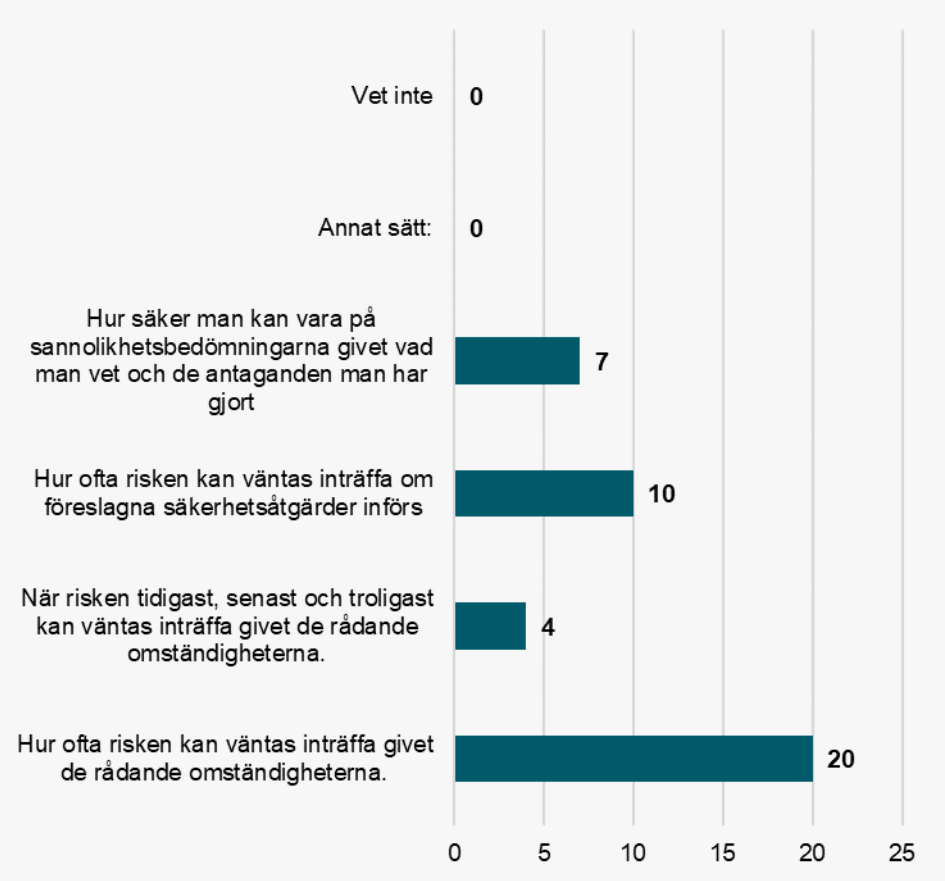
Av svaren på fråga 36 framgår att ansvaret för identifierade informationsrisker ligger på Informationsägare (17 regioner) och på Riskägare (elva regioner). Fem regioner har svarat att ansvaret ligger på t.ex. Informationssäkerhetssamordnare, Verksamhetschef eller Objektägare.

Figur 33 [37] Vad avgör om en informationssäkerhetsrisk ska accepteras eller åtgärdas?



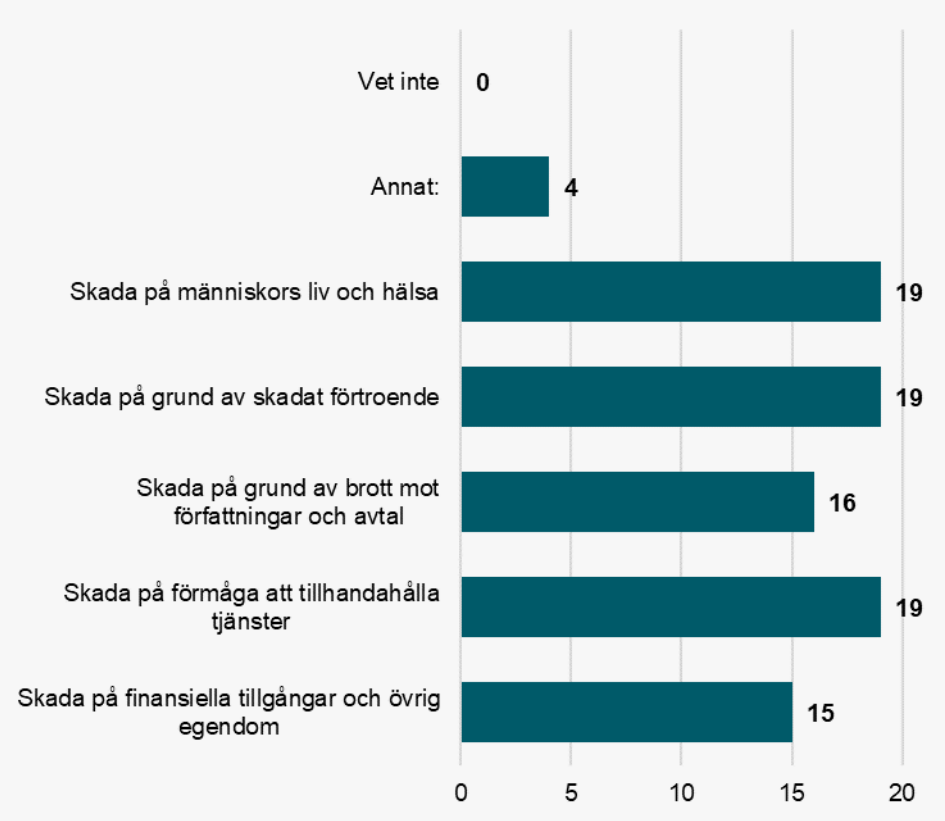
Av svaren på fråga 37 framgår att 13 regioner svarat att det är riskens sannolikhet och konsekvens som avgör om en risk ska accepteras eller åtgärdas. I nio av regionerna är det riskvärde jämfört med beslutade intervall som är avgörande. I något färre regioner (fem stycken) är det ekonomiskt ansvarig för den aktuella verksamheten som avgör om risken ska accepteras eller åtgärdas.

Figur 34 [38] Vad vägs in vid sannolikhetsbedömningar för informationssäkerhetsrisker?



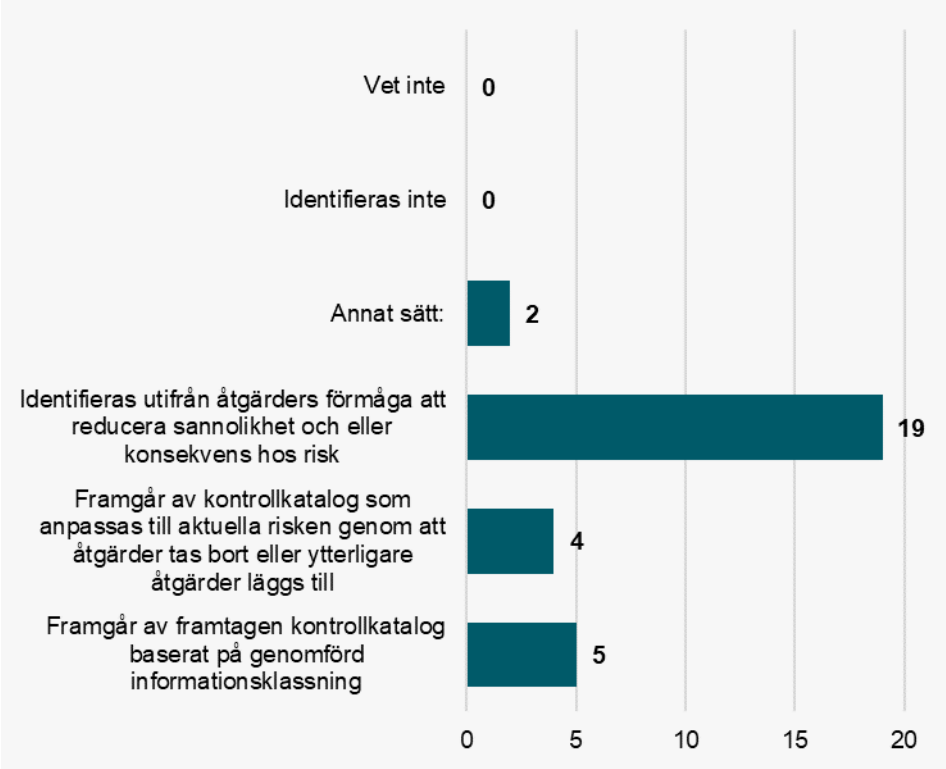
Av svaren på *fråga 38* framgår att 20 av 20 svarade regioner väger in hur ofta, d.v.s. med vilken frekvens, en risk väntas inträffa. Av 20 svarade regioner väger tio in effekten av om föreslagna säkerhetsåtgärder införs, sju regioner väger in hur säker man kan vara på gjorda sannolikhetsbedömningar och fyra regioner anger sannolikheten i form av ett trepunktsestimat.

Figur 35 [39] Vad vägs in vid bedömning av skadeverkan/konsekvens för informationssäkerhetsrisker?



Av svaren på *fråga 39* framgår att 19 av 20 svarade regioner väger in skada på människors liv och hälsa, skada på förtroende samt skada på förmåga att tillhandahålla tjänster vid bedömning av skadeverkan/konsekvens för risken. Skada på finansiella tillgångar samt på grund av brott mot författningar och avtal ges en något lägre betydelse, dock har även dessa en tydlig representation.

Figur 36 [40] Hur identifieras riskreducerande åtgärder?



Av svaren på *fråga 40* framgår att 19 av 20 svarande regioner identifierar riskreducerande åtgärder utifrån åtgärders förmåga att reducera sannolikhet och/eller konsekvens hos risken. Fem av 20 svarande regioner anger att riskreducerande åtgärder framgår av framtagen kontrollkatalog baserat på genomförd informationsklassning. Fyra av 20 svarande regioner anger att riskreducerande åtgärder framgår av framtagen kontrollkatalog och där angivna kontroller anpassas till den aktuella risken.

Figur 37 [41] Hur sker uppföljning av riskreducerande åtgärder?

Av svaren på *fråga 41* framgår att 14 av 20 svarande regioner följer upp genom att granska att de riskreducerande åtgärderna är implementerade. Sex av 20 svarade regioner följer upp genom att granska åtgärdernas förmåga att reducera sannolikhet respektive att reducera konsekvens.

Iakttagelser

20 av 21 regioner har ett beslutat arbetssätt för hantering av informations-säkerhetsrisker vilket kan jämföras med 13 av 20 i MSB:s rapport från 2018.

Jämfört med MSB:s rapport från 2018 utförs riskanalyser på ett bredare spektrum av händelser än bara IT-relaterade händelser. Tyngden ligger fortfarande på IT-relaterade händelser men det bredare spektrumet vid denna uppföljning tolkas som ökad mognad och förståelse för att informations-säkerhetsarbetet omfattar betydligt mer än IT-nära verksamhet.

Vid bedömning av sannolikhet att en risk inträffar svarar samtliga 20 regioner att hänsyn tas till de rådande omständigheterna, sju regioner väger även in hur säker man är på att bedömningen i sig är korrekt och fyra regioner anger sannolikheten i form av ett trepunktsestimat.

Majoriteten av regionerna (19 av 20) identifierar riskreducerande åtgärder utifrån åtgärders förmåga att reducera sannolikhet och/ eller konsekvens hos risken. Hos fem av 20 regioner framgår åtgärderna av framtagen kontrollkatalog. Hos fyra av 20 regioner tillämpas en tvåstegsmetod där åtgärder först framgår av framtagen kontrollkatalog och därefter anpassas till den aktuella risken.

Utbildning

Beskrivning av området

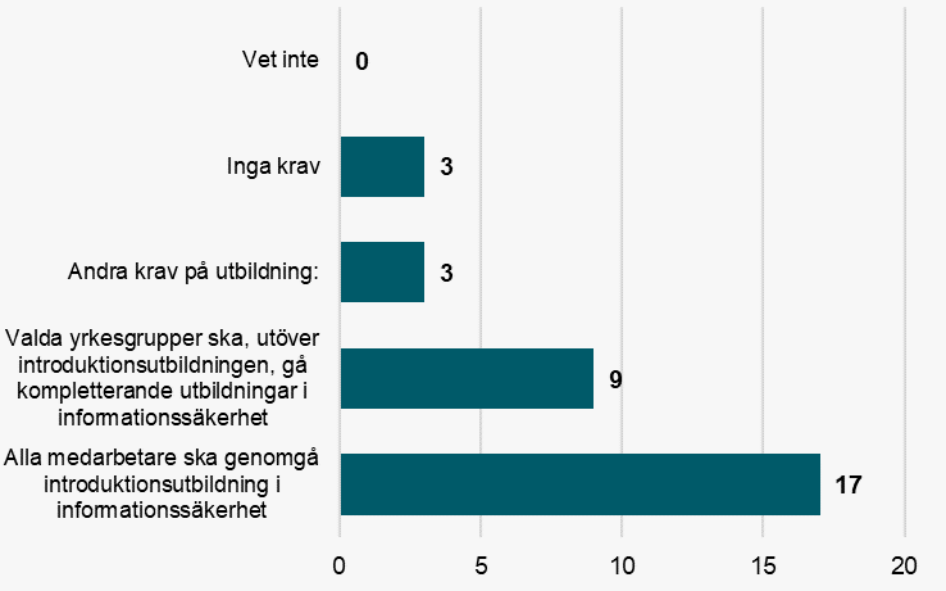
Inom detta uppföljningsområde avses i första hand utbildning inom informationssäkerhet.

Utbildning är en väsentlig del i att upprätthålla en god nivå i informationssäkerhetsarbetet och för att bygga upp en god säkerhetskultur.

Utbildningar behöver anpassas till såväl arbetsuppgifter som den befintliga kompetensnivån i organisationen. Det gäller särskilt de funktioner och roller med utpekade uppgifter för organisationens informationssäkerhetsarbete.

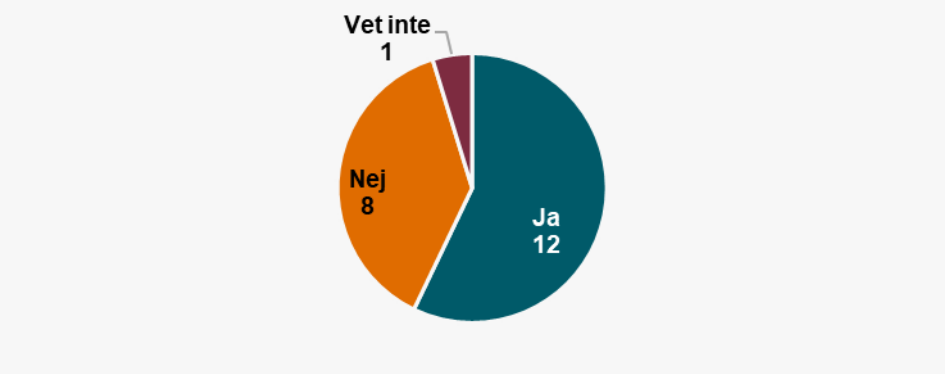
Erhållna svar

Figur 38 [43] Vilka krav har regionen på utbildning inom informationssäkerhet för medarbetare inom hälso- och sjukvårdsverksamheten?



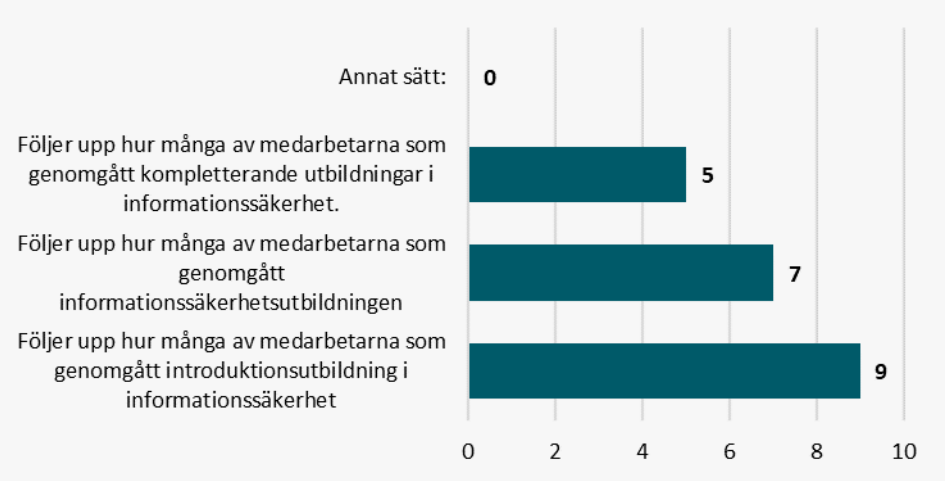
Av svaren på *fråga 43* framgår att 17 av de 21 svarande regionerna har krav på att alla medarbetare ska genomgå introduktionsutbildning i informations-säkerhet. Nio av de svarande regionerna angav att valda yrkesgrupper därutöver ska gå kompletterade utbildningar. Tre av de svarande regionerna hade andra krav på utbildning och tre av regionerna hade inga krav på utbildning.

Figur 39 [44] Följer regionen upp genomförda utbildningar om informationssäkerhet för medarbetare inom hälso- och sjukvårdsverksamheten?



Av svaren på *fråga 44* framgår att tolv av de 21 svarande regionerna följer upp genomförda utbildningar medan åtta regioner inte följer upp genomförda utbildningar.

Figur 40 [45] Hur följer regionen upp genomförd utbildning om informationssäkerhet för medarbetare inom hälso- och sjukvårdsverksamheten?



Av svaren på *fråga 45* framgår att av de tolv regioner som följer upp genomförda utbildningar så följer nio regioner upp genomförd introduktionsutbildning medan de för övriga utbildningar ligger på en något lägre nivå.

Iakttagelser

17 regioner ställer krav på att samtliga medarbetare ska genomföra en grundläggande informationssäkerhetsutbildning, och ska jämföras med tio regioner som hade samma krav i MSB:s rapport från 2018.

Det går att se motsvarande utveckling vad gäller kravet att valda yrkesgrupper därutöver ska gå kompletterade utbildningar, här har siffran ökat från tre till nio.

I denna mätning framgår även att tolv av regionerna följer upp utbildningsinsatserna inom informationssäkerhetsområdet, detta är en ökning från MSB:s rapport från 2018 då åtta regioner genomförde uppföljning.

Uppföljning av genomförda utbildningar är ett område som flera regioner uppgett som ett fokusområde för de närmaste åren.

Upphandling och utveckling

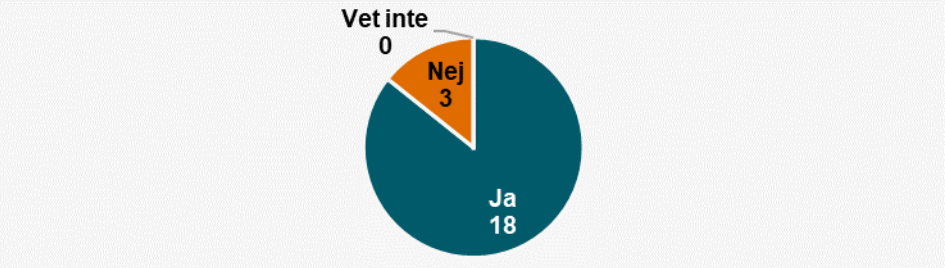
Beskrivning av området

Inom detta uppföljningsområde avses i första hand upprättande och användande av informationssäkerhetsrelaterade krav vid upphandlingar och utveckling.

Ett systematiskt arbetssätt behöver tillämpas vid upphandling av produkt eller tjänst. Arbetssättet behöver omfatta såväl att kunna ställa korrekta informationssäkerhetskrav på produkten/tjänsten som att kunna verifiera att ställda informationssäkerhetskrav är uppfyllda.

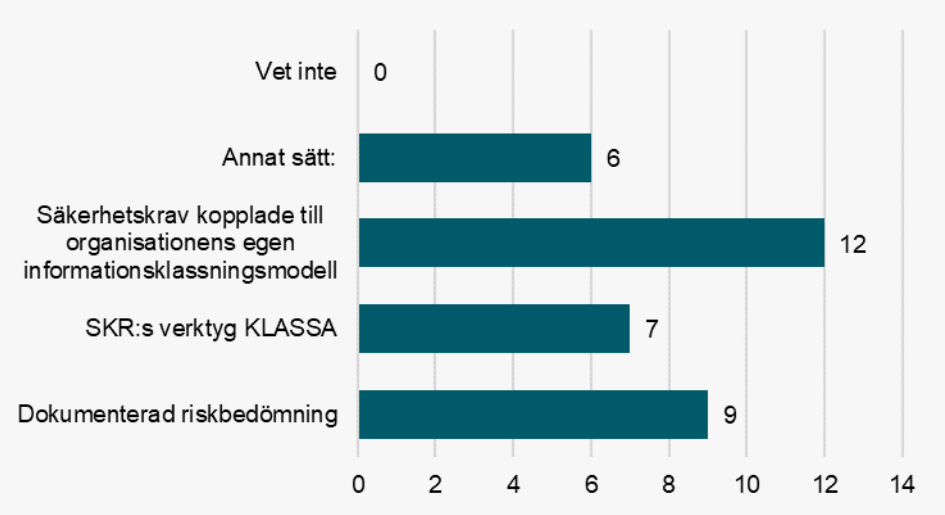
Erhållna svar

Figur 41 [47] Finns ett beslutat arbetssätt för att ställa informationssäkerhetskrav vid upphandlingar och vid systemutveckling inom hälso- och sjukvårdsverksamheten?



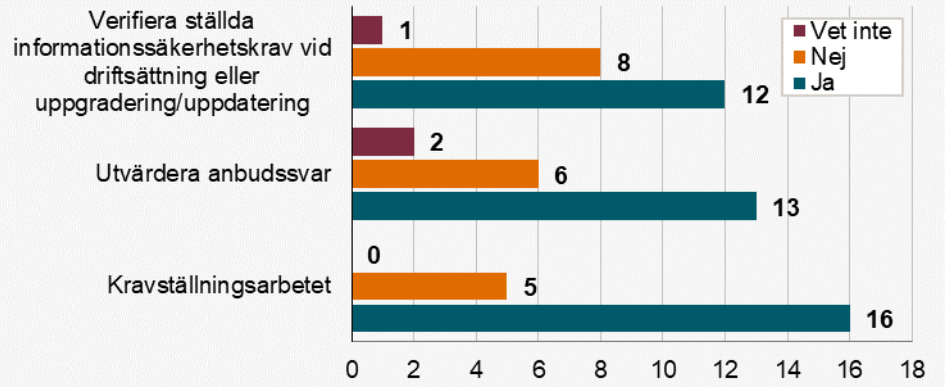
Av *fråga 47* framgår att 18 av 21 svarande regioner har ett beslutat arbetssätt där informationssäkerhetskrav ställs vid upphandlingar och systemutveckling.

Figur 42 [48] Vad ingår i det beslutade arbetssättet för att ställa informationssäkerhetskrav vid upphandlingar och vid systemutveckling?



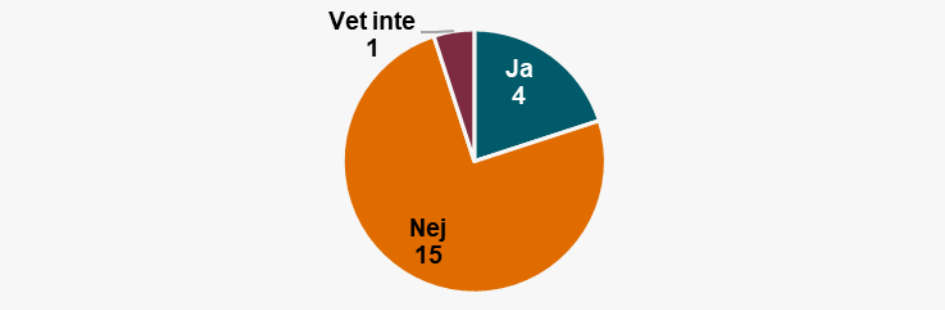
Av *fråga 48* framgår att tolv av 21 svarande regioner baserar informationssäkerhetskrav på koppling till informationssäkerhetsklassning. Nio regioner anger att dokumenterad riskbedömning ingår i det beslutade arbetssättet. Hos sju regioner ingår verktyget KLASSA i det beslutade arbetssättet.

Figur 43 [49.1] Finns ett beslutat arbetssätt inom hälso- och sjukvårdsverksamheten för att få med informationssäkerhetskompetens vid följande moment vid it-relaterade upphandlingar? Kravställningsarbetet. [49.2] Finns ett beslutat arbetssätt inom hälso- och sjukvårdsverksamheten för att få med informationssäkerhetskompetens vid följande moment vid it-relaterade upphandlingar? Utvärdera anbudssvar. [49.3] Finns ett beslutat arbetssätt inom hälso- och sjukvårdsverksamheten för att få med informationssäkerhets-kompetens vid följande moment vid it-relaterade upphandlingar? Verifiera ställda informationssäkerhetskrav vid driftsättning eller uppgradering/uppdatering.



Av *frågorna 49.1, 49.2 och49.3* framgår att 16 av 21 regioner har med informationssäkerhetskompetens i kravställningsarbetet, 13 regioner har med informationssäkerhetskompetens när anbudssvar ska utvärderas och tolv regioner har med informationssäkerhetskompetens när kravuppfyllnad ska utvärderas.

Figur 44 [50] Finns ett beslutat arbetssätt inom hälso- och sjukvårdsverksamheten för att under kontraktstiden granska avtalade säkerhetsåtgärder som framgår av avtalet?



Av *fråga 50* framgår att endast fyra av 20 svarade regioner har ett beslutat arbetssätt för att granska avtalade säkerhetsåtgärder under kontraktstiden.

Iakttagelser

Antalet regioner som har ett beslutat arbetssätt för att ställa informationssäkerhetskrav vid upphandlingar och systemutveckling har ökat från 15 av 20 landsting/regioner i MSB:S rapport från 2018 till 18 av 21 regioner vid denna uppföljning.

När det gäller att få med informationssäkerhetskompetens vid upphandlingssituationer ligger tyngdpunkten vid kravställning (16 regioner) medan utvärdering av anbudsvar och utvärdering av kravuppfyllnad är lägre (13 respektive tolv regioner).Detta tydliggörs ytterligare vid jämförelse av utfallen från fråga 47 och fråga 50. 18 av 21 regioner har ett beslutat arbetssätt för att ställa informationssäkerhetskrav vid upphandlingar och systemutveckling medan endast fyra av 20 svarade regioner har ett beslutat arbetssätt för att granska avtalade säkerhetsåtgärder under kontraktstiden.

Trots denna obalans kan dock en viss positiv trend identifieras då det i MSB:s rapport från 2018 endast var en av 20 landsting/regioner som uppgav att det fanns ett beslutat arbetssätt för att granska avtalade säkerhetsåtgärder under kontraktstiden.

Utkontrakterade (outsourcade) it-tjänster, inklusive molntjänster

Beskrivning av området

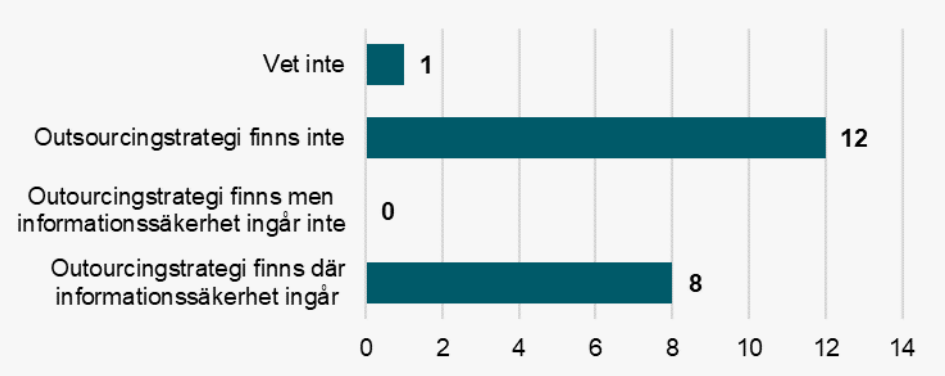
Inom detta uppföljningsområde avses i första hand utkontraktering av drift av informationstjänster och huruvida detta sker med beaktande av informationssäkerhet.

Exempel på faktorer som kan behöva vägas in är behovet av att identifiera risker som uppkommer i samband med outsourcing och att i en sourcingpolicy göra avdömning gällande riskacceptansen.

För beslut och för planering av tjänster samt för att bedöma utifall utkontraktering kan vara accepterat behöver ledning och verksamhet ha denna övergripande riskbedömning som ett beslutsunderlag.

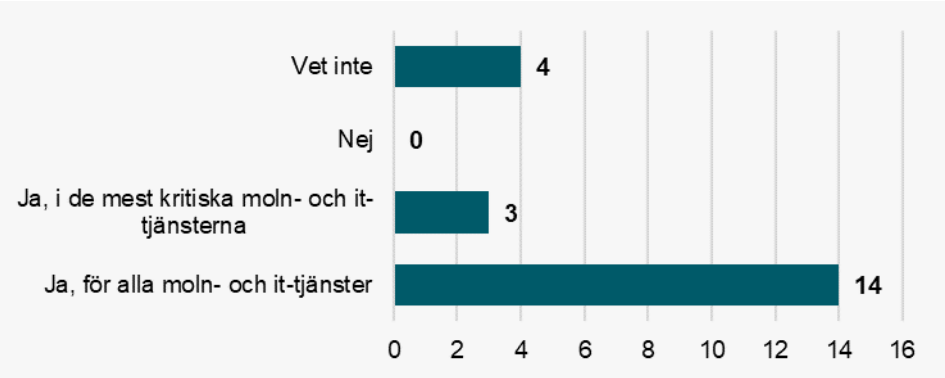
Erhållna svar

Figur 45 [52] Har regionens hälso- och sjukvårdsverksamhet en outsourcingstrategi där informationssäkerhet ingår?



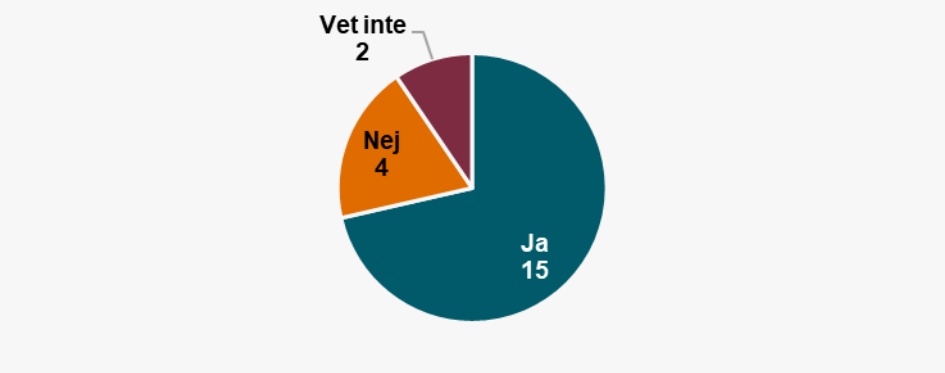
Av *fråga 52* framgår att tolv av 21 svarande regioner inte har någon outsourcingstrategi. Hos de åtta regioner som har en outsourcingstrategi så inkluderar denna strategi informationssäkerhet.

Figur 46 [53] Har regionens hälso- och sjukvårdsverksamhet krav på att leverantör av molntjänster och utkontrakterade (outsourcade) it-tjänster ska rapportera it-incidenter i berörda system till regionen?



Av fråga 53 framgår att 17 av 21 svarande regioner har krav på att leverantörer rapporterar IT-incidenter.

Figur 47 [54] Har regionen någon upphandlad molntjänst som är nödvändig för en eller flera verksamhetskritiska processer inom hälso- och sjukvårdsverksamheten?



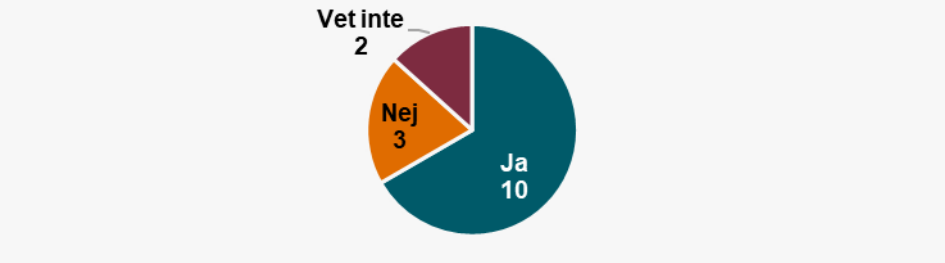
Av svaren på *fråga 54* kan det konstateras att 15 av de svarande regionerna upphandlar molntjänster som är nödvändiga för verksamhetskritiska processer.

Figur 48 [55] Vilka är de huvudsakliga anledningarna till att molntjänster används inom hälso- och sjukvårdsverksamheten?

Enligt svaren på *fråga 55* är de viktigaste anledningarna till användning av molntjänster ökad flexibilitet och kostnadsfördelar följt av att möjliggöra fokus på organisationens huvuduppgifter och underlätta mjukvaruhantering.

Utöver dessa svar behöver svarsalternativet ”Annan anledning” lyftas fram då givna förklaringar här så gott som uteslutande beskrev att regionerna inte hade några alternativ till molntjänster då leverantörerna inte erbjöd en lösning för ”on-prem”.

Figur 49 [56] Ställer regionen krav på ett beslutat och infört ledningssystem för informationssäkerhet hos leverantörer av molntjänster och utkontrakterade (outsourcade) it-tjänster som används i verksamhetskritiska processer inom hälso- och sjukvårdsverksamheten?



Av svaren på *fråga 56* framgår att tio av de regioner som svarade ”Ja” på fråga 54 (15 st.) även ställde krav på att leverantören skulle ha ett beslutat och infört LIS.

Iakttagelser

Det är åtta regioner som har en outsourcingstrategi och i samtliga fall är informationssäkerhet inkluderat i strategin. Det är en klar ökning från MSB:s rapport från 2018, då endast tre landsting/regioner uppgav att det fanns en outsourcingstrategi med informationssäkerhet inkluderat.

För att utveckla det systematiska och riskbaserade informationssäkerhetsarbetet är det väsentligt att ha koll på incidenterna. I denna uppföljning är det 14 regioner som ställer krav på leverantörerna att rapportera incidenter jämfört med nio i MSB:s rapport från 2018.

Det är 15 regioner som uppger att de upphandlar molntjänster som är nödvändiga för verksamhetskritiska processer (som exempel insulinpumpar och olika MT-utrustningar), denna siffra ska jämföras med sex i MSB:s rapport från 2018.

De huvudsakliga anledningarna till att regionerna använder molntjänster inom hälso- och sjukvårdsverksamheten varierar, men de som lyfts fram är kostnadsfördelar, ökad flexibilitet och att befintliga lösningar går över till molntjänster.

Det är inte bara viktigt att upphandlade lösningar uppfyller regionernas krav på informationssäkerhet, det är lika viktigt att leverantören arbetar systematiskt och riskbaserat med sitt informationssäkerhetsarbete. I denna uppföljning

framgår att tio regioner ställer krav på ett beslutat och infört ledningssystem för informationssäkerhet hos leverantörer av molntjänster och outsourcade IT-tjänster.

Incidenter som påverkar informationshantering

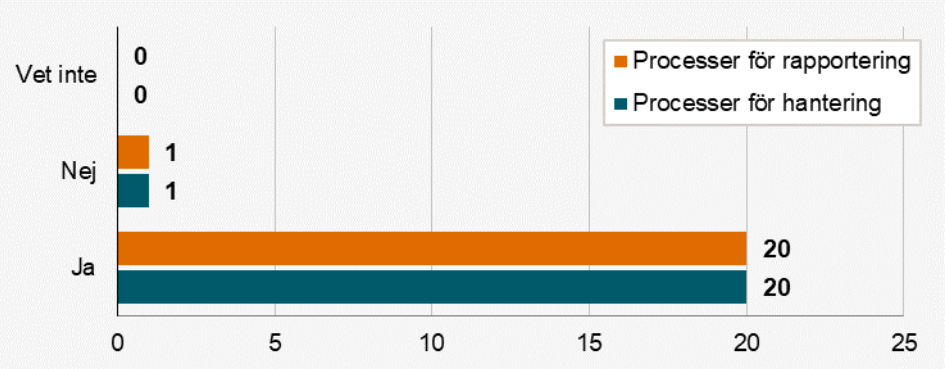
Beskrivning av området

Ett systematiskt arbete med rapportering och hantering av incidenter fyller flera syften. Det ger en förbättrad möjlighet att få ett rättvisande underlag för arbetet med analyser av organisationens risker vilket i sin tur underlättar att vidta rätt förebyggande åtgärder.

Vidare är det av vikt för kontinuitetsplaneringen eftersom det även här bidrar till förståelsen av vilka verksamheter som är särskilt utsatta för incidenter, på vilket sätt detta sker och vilka risker som behöver hanteras inom ramen för kontinuitetsplaneringen.

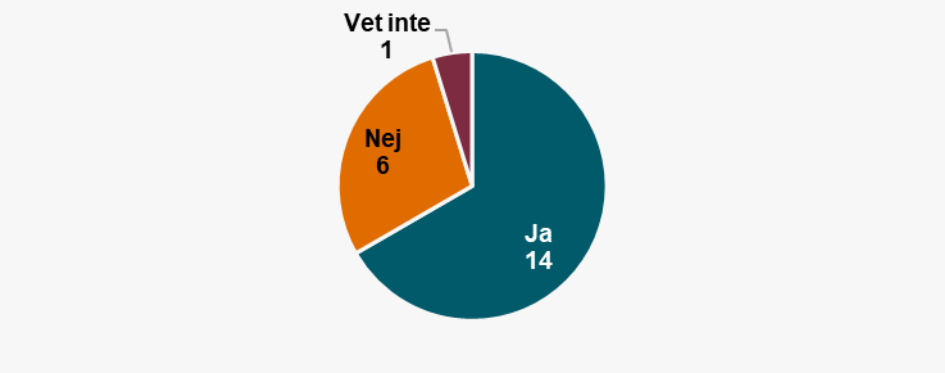
Erhållna svar

Figur 50 [58.1] Har regionen processer för intern rapportering och hantering av informationssäkerhetsincidenter inom hälso- och sjukvårdsverksamheten som inte har klassats som patientsäkerhetsincidenter? **Processer för rapportering.**
[58.2] Har regionen processer för intern rapportering och hantering av informationssäkerhetsincidenter inom hälso- och sjukvårdsverksamheten som inte har klassats som patientsäkerhetsincidenter? **Processer för hantering.**



Av svaren på *fråga 58.1* och *fråga 58.2* kan konstateras att det hos 20 av 21 svarande regioner finns processer för såväl rapportering som hantering av informationssäkerhetsincidenter.

Figur 51 [59] Finns det möjlighet för den som har det övergripande ansvaret för samordning av informationssäkerhetsarbetet att utan begränsningar ta del av samtliga rapporterade incidenter/avvikelser inom hälso- och sjukvårdsverksamheten, oavsett kategorisering?



Av svaren på *fråga 59* kan konstateras att det hos 14 av 21 svarande regioner finns möjlighet för rollen som ansvarar för samordning av informationssäkerhetsarbetet att ta del av rapporterade incidenter.

Iakttagelser

Antalet regioner som har processer för intern rapportering respektive för hantering av informationssäkerhetsincidenter har ökat från 15 av 20 i MSB:s rapport från 2018 till 20 av 21 vid denna uppföljning, detta får anses vara en tydlig förbättring.

Antalet regioner där rollen med det övergripande ansvaret för samordning av informationssäkerhetsarbetet att utan begränsningar kan ta del av samtliga rapporterade incidenter/avvikelser inom hälso- och sjukvårdsverksamheten har ökat från tio landsting/regioner i MSB:s rapport från 2018 till 14 regioner vid denna uppföljning.

Regionernas informationssäkerhetsarbete

Ett lyckat införande av ett systematiskt och riskbaserat informationssäkerhetsarbete hänger samman med ledningens aktiva engagemang.

Under vintern/våren 2021/2022 genomförde SKR en webbenkät om hur långt regionerna kommit i sitt systematiska informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten.

Det finns en djupare och bredare förståelse av hur viktigt ett grundläggande systematiskt och riskbaserat informationssäkerhetsarbete är för den fortsatta digitaliseringen av hälso- och sjukvården.

Denna publikation vänder sig till både ledning och CISO i regionerna.

Upplysningar om innehållet
Jonas Nilsson, jonas.nilsson@skr.se

ISBN/Beställningsnummer: 978-91-8047-082-7
Text: Jonas Nilsson

ISBN 978-91-8047-082-7
Beställ eller ladda ner på webbutik.skr.se
Post: 118 82 Stockholm | **Besök:** Hornsgatan 20
Telefon: 08-452 70 00 | www.skr.se

Sveriges Kommuner och Regioner