Informationssäkerhetsberättelse 2024

Sammanfattning

Regionens arbete med informationssäkerhet syftar till att stödja det övergripande målet att rätt information når rätt person i rätt tid. Detta bidrar till en välfungerande verksamhet där regionen når sina mål från våra uppdragsgivare och till våra medborgare.

Det försämrade säkerhetsläget och ett ökat cybersäkerhetshot innebär att vi har en fortsatt förhöjd övergripande hotnivå. Detta ser vi inte minst i att offentlig verksamhet med hälso- och sjukvårdssektorn utgör prioriterade måltavlor för dessa hot.

Informationssäkerhetsfunktionen har under 2024 arbetat med att uppnå till en förmågehöjning av informationssäkerhetsarbetet utifrån MSB:s metodstöd och standardiserade arbetssätt utifrån området informationssäkerhet.

Denna eftersträvade förmågehöjning har inte kunnat realiseras vilket reflekteras i nyckeltalen som presenteras nedan. De huvudsakliga faktorerna till detta är framför allt att det etablerade sättet arbetet idag utförs på sker decentraliserat utan kvalitetssäkrat koordinerat samarbete. Vidare framkommer brister i mandat kopplade till nyckelroller inom säkerhetsområdet vilket visar sig som brister i avsaknad av kontinuerlig rapportering till både organisationens tjänstemannaledning såväl som politiska ledning. Detta medför att organisationsövergripande beslut för att säkerställa skyddet för organisationen uteblivit. Exemplifierat genom att det inte finns en systematik att rapportera identifierade risker som kräver skyndsamma åtgärder samt ledningsbeslut. Beslut som ofta saknar delegerade rättigheter att besluta om hos befintliga medarbetare som arbetar inom säkerhetsområdet i organisationen idag.

Informationssäkerhetsberättelse 2024

Informationssäkerhetsberättelsen beskriver Region Jämtland Härjedalens arbete inom områdena informationssäkerhet för det gångna verksamhetsåret

Utifrån vad som presenterades vid förra årets informationssäkerhetsberättelse och den informationssäkerhetspolicy som fastställdes av Regionfullmäktige 2024 kommer rapporteringen att ske i form av nyckeltal baserade på de målområden som där definierats.

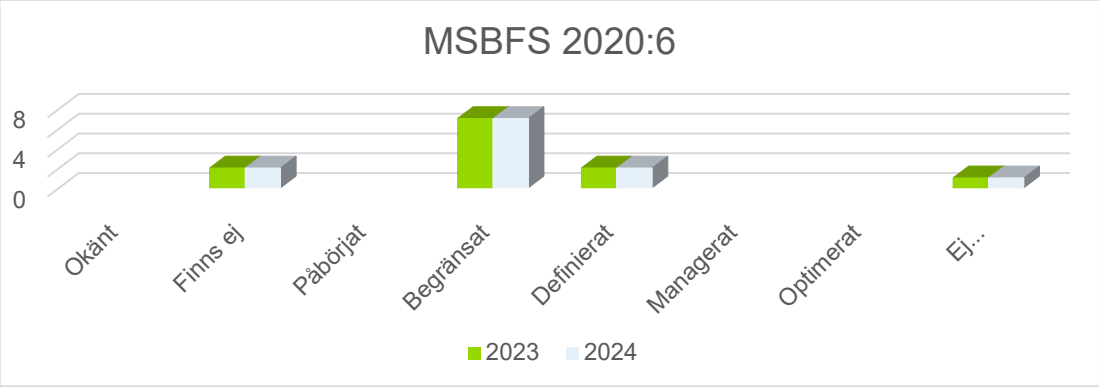
Nyckeltal

Nyckeltalen är utformade utifrån de mål som identifierats och fastställt i Region Jämtland Härjedalens informationssäkerhetspolicy.

Ledningssystem för informationssäkerhet	• Procent av efterlevnad av MSBFS 2020:6 12 kravområden
Riskhantering	• Mognadsnivå utifrån MSB:s Cybersäkerhetskollen • Sammanfattning av övergripande riskanalys utifrån omvärldsbevakning • Procent av genomförda riskanalyser utifrån identifierade verksamhetskritiska områden • Sammanfattning av informationssäkerhetsrisker ur riskregistret
Informationssäkerhetsorganisation	• Tillsatta roller, tilldelade mandat samt resurser
Informationsklassning	• Procent av genomförda informationsklassningar på antal aktuella informationssystem
Informationssäkerhetsutbildning	• Procent av medarbetare som genomfört 2024 års informationssäkerhetsutbildning

Måluppfyllnad utifrån nyckeltal

Nyckeltal: Ledningssystem för informationssäkerhet (LIS)



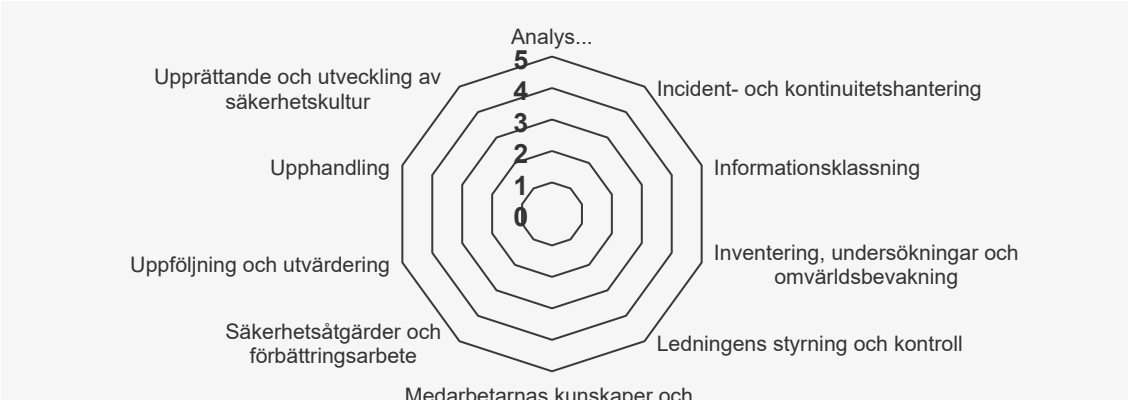
Figur 1 Trend efterlevnad av MSBFS 2020:6

Status	Innebörd
Okänt	Har ännu ej kontrollerats
Finns ej	Helt avsaknad av känd styrning, processer, rutiner
Påbörjat	Har påbörjats
Begränsat	Fortskrider som planerat men ännu ej klart
Definierat	Dokumenterat men ännu ej implementerat, kommunicerat eller fungerande
Managerat	Har precis börjat användas
Optimerat	Används, fungerar och följs upp regelbundet
Ej applicerbart	Ej Applicerbart för verksamhet

Figur 2 Förklaring av nivåerna för efterlevnad Figur 1

Nyckeltal	Rapportering	Kommentar	Förslag
Procent av efterlevnad av MSBFS 2020:6 12 kravområden	Inga framsteg har gjorts på området sedan föregående rapportering	Även om vissa förbättringar genomförts inom informationssäkerhetsområdet finns det idag inte förutsättningar för att efterleva de informationssäkerhetskrav vi som organisation har på oss. De huvudsakliga faktorerna till detta är framför allt att det etablerade sättet arbetet idag utförs på sker decentraliserat utan kvalitetssäkrat koordinerat samarbete. Även brister i mandat kopplade till nyckelroller inom säkerhetsområdet	Förslag på ny säkerhetsorganisation har beställts av Regiondirektören (RS/754/2024) som ska kunna tillgodose ett adekvat säkerhetsarbete. Eventuellt genomförande av förslaget bedöms innebära kostnadsreduceringar, högre lagefterlevnad, ökat stöd för verksamheten, samt en minskning av de risker regionen lever med idag

Nyckeltal: Riskhantering



Figur 3 Mognadsnivå utifrån MSB:s Cybersäkerhetskollen 2024

Nyckeltal	Rapportering	Kommentar	Förslag
Mognadsnivå – MSB: Cybersäkerhetskollen	Regionens genomsnitt är 0,8 på den 5 gradiga skalan	Den låga mognaden tyder på till stora delar avsaknad av strukturerat informationssäkerhetsarbete	Förslag på ny säkerhetsorganisation arbetas med för att åstadkomma en förmågehöjning av säkerhetsarbetet och organisationens robusthet

Nyckeltal	Rapportering	Kommentar	Förslag
Sammanfattning av övergripande riskanalys utifrån omvärldsanalys	Ingen övergripande riskanalys har genomförts	Ingen övergripande riskanalys har genomförts då nuvarande arbete med stora brister i	Förslag på ny säkerhetsorganisation arbetas med för att förtydliga roller,

		samordning inte möjliggör denna typ av aktivitet	ansvar och samarbetsformer

Nyckeltal	Rapportering	Kommentar	Förslag
Procent av genomförda riskanalyser utifrån identifierade verksamhetskritiska områden	Riskanalyser är till viss del genomförda i systemstödet Stratsys men inte utifrån verksamhetskritiska områden	Verksamhetskritiska områden, processer och information har inte identifierats vilket omöjliggör dessa riktade riskanalyser	Dokumentera organisationens kärn- och stödprocesser för att utifrån det underlaget identifiera vilka områden som är verksamhetskritiska

Nyckeltal	Rapportering	Kommentar	Förslag
Sammanfattning av informationssäkerhets-risker ur riskregistret	4 kritiska 9 höga 8 medel 4 låga	Regionen saknar idag ett enhetligt riskramverk och rollen riskansvarig för ett strukturerat och fungerande riskarbete vilket inte möjliggör rapportering inom området	Förslag på ny säkerhetsorganisation arbetas med för att åstadkomma ett strukturerat säkerhetsarbete där rollen riskansvarig kan utbilda, följa upp och rapportera riskarbetet

Nyckeltal: Informationssäkerhetsorganisation

Nyckeltal	Rapportering	Kommentar	Förslag
Tillsatta roller, mandat och resurser	Stort antal medarbetare (ca. 50 st) som arbetar direkt inom säkerhetsrelaterade roller	Det saknas tydligt definierade roller och ansvar, vilket leder till att mandat inom säkerhetsarbetet saknas, att ledningens involvering saknas, samt att flera kritiska områden inte omhändertas. Nuvarande roller arbetar nästan uteslutande på operativ nivå vilket ger att strategiskt framåtsyftande arbete brister	Förslag på ny säkerhetsorganisation arbetas med för att åstadkomma ett strukturerat säkerhetsarbete med motsvarande 12 medarbetare som genom ett strukturerat och systematiskt säkerhetsarbete, med tydliga roller och ansvar, kravställer, följer upp samt rapporterar till ledningen löpande

Förslag på ny säkerhetsorganisation är under uppstart (RS/754/2024). Ingångsvärdet är att efterlikna en säkerhetsorganisation som är vedertagen inom kommuner och regioner med säkerhets- och juridikavdelning på uppskattningsvis drygt 10-12 medarbetare med tydlig ansvarsfördelning, uppföljning och återrapportering till ledningen.
Syftet med arbetet är att ge ekonomiska besparingar, högre lagefterlevnad, ökat stöd för verksamheten samt en omfattande minskning av de risker regionen lever med idag.

Som jämförelse kan beskrivas att inom privat sektor i en organisation i motsvarande storlek som Region Jämtland Härjedalen återfinns normalt sett endast 4 roller för att täcka säkerhetsbehoven: CISO (Chief Information Security Officer), CRO (Chief Risk Officer), CCO (Chief Compliance Officer) och DSO (Dataskyddsombud). Till jämförelsen skall tilläggas att kraven på organisationer i privat kontra offentlig sektor skiljer sig åt varpå en säkerhetsorganisation i offentlig sektor uppskattas utgöras av något fler roller och medarbetare.

Nyckeltal: Informationsklassning

Nyckeltal	Rapportering	Kommentar	Förslag
Procent av genomförda informationsklassningar på antal aktuella informationssystem	30 informationsklassningar genomfördes strukturerat under 2024	Då antalet informationssystem är okänt (3000+) och regionen inte har en ändamålsenlig utvecklings- och inköpsprocess kan vi inte rapportera på detta nyckeltal	Identifiera och sätt ägarskap över regione samtliga Informations- Kommunikationstekno (IKT)

Nyckeltal: Informationssäkerhetsutbildning

Nyckeltal	Rapportering	Kommentar	Förslag
Procent av medarbetare som genomfört 2024 års informationssäkerhetsutbildning	Av ca 5200 identifierad medarbetare har 2555 medarbetare inte slutfört 2024 års informationssäkerhetsutbildning. Detta ger en procentsats på strax under 50 procent som genomfört utbildningen. Nytt för årets utbildning är formatet microlearning som genomförts i flera korta interaktiva e-moduler	Även om vi ser en markant ökning från tidigare år så finns det ett stort utrymme för förbättring inom området	Ökad uppföljning under 2025, med särskilt fokus på områdena Hälsocentral Folktandvård och förtroendeva

Slutsats

Sedan senaste rapporteringen har huvudfokus inom informationssäkerhetsarbetet varit att förankra rollen som CISO (informationssäkerhetsansvarig), finnas som stöd för regionens verksamheter samt att utveckla ett centraliserat koordinerat samarbete inom informationssäkerhetsarbetet med angränsande berörda säkerhetsfunktioner. Ramverket till ett LIS (Ledningssystem för informationssäkerhet) finns framtagen men har ännu ej beslutats då samverkansformer med alla berörda parter inte etablerats.

Detta leder till att det idag därför inte finns organisatoriska förutsättningar för att bedriva ett strukturerat och kvalitativt säkerhetsarbete i enlighet med de lagrum som styr vårt uppdrag och hur omvärldsläget ser ut. Vilket återspeglas i rapporteringen i nyckeltalen i denna rapport.

Ett förslag har lagts fram där man föreslår att arbeta strategiskt, tillsätta medarbetare utifrån adekvat utbildning och erfarenhet, samt basera arbetet utifrån erkända nationella standarder och etablerade arbetsformer inom området. Förslaget bedöms innebära reducerade kostnader för säkerhetsarbetet inom regionen, ge högre lagefterlevnad, ökat och förenklat stödet till verksamheterna samt minska de risker regionen lever med idag.

Det beskrivna arbetet att initialt ta fram ett förslag för att sedan kunna etablera en ny säkerhetsorganisation i organisationen emfaseras. Detta då det stora behovet av att komma till rätta med säkerhetsarbetet i organisationen måste beskrivas som direkt avgörande för organisationens resiliens och förmåga att leverera mot sitt samhällsuppdrag nu och framåt över tid. Vidare så bedöms organisationsledningens involvering och ägarskap som avgörande för att lyckas med den förflyttning som detta innebär.