REGION JÄMTLAND HÄRJEDALEN

N/A
Dan Alonso
Tfn:
E-post:

2024-03-04

RS/95/2024

Informationssäkerhetsberättelse 2023

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 har höjt den övergripande hotnivån ytterligare under 2023. Detta ser vi inte minst i att offentlig verksamhet med hälso och sjukvårdssektorn framför allt som måltavlor för dessa grupper.

Informationssäkerhetsfunktionen har fått en ny informationssäkerhetsansvarig under senare delen av 2023 vilket lett till en nystart och större standardisering av informationssäkerhetsarbetet på regionen. Det nya arbetssättet utgår från MSB:s metodstöd och bästa praxis utifrån området informationssäkerhet.

Det nya arbetssättet kommer även innebära att vi nu kan börja mäta och följa upp arbetet på ett helt annat sätt än vi tidigare gjort. Detta kommer att göras utifrån de fem övergripande målen som identifierats i regionens informationssäkerhetspolicy.

Den nya informationssäkerhetsansvarige har inte tillräckligt underlag för att påvisa vad tidigare anställd på tjänsten gjort under 2023 då det arbetet i stort bedrevs operativt

Den största utmaningen inom området är den decentralisera arbetskulturen som finns idag på regionen och som gör mätning och uppföljning väldigt utmanande. Här behöver vi i stället se vilka delar som kan centraliseras för att skapa enhetliga processer och rutiner över regionen som i sin tur kan följas upp och förbättras kontinuerligt.

1. Informationssäkerhetsberättelse 2023

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

Då informationssäkerhetsfunktionen har fått en ny informationssäkerhetsansvarig har det påbörjats en nystart inom området. Dels kommer funktionen att arbeta mer strategiskt där samarbete med andra säkerhetsfunktioner är en förutsättning, dels kommer arbetet att struktureras i enlighet med MSB:s metodstöd[1] som är en de facto standard inom offentlig sektorn.

[1] https://www.informationssakerhet.se/metodstodet/

Tidigare arbetssätt	Nytt arbetssätt
• Informationssäkerhetssamordnare som arbetar operativt • Tidigare rapportering utifrån tre+ områden • De-centarliserat säkerhetsarbete • Otydliga roller och mandat	• Informationssäkerhetsansvarig som arbetar strategiskt • Ny rapportering utifrån de fem målen i informationssäkerhetspolcyn • Centraliserat säkerhetsarbete • Tydliga roller och mandat

Figur 1 nuläge gentemot målbild

2. Rapportering av nyckeltal

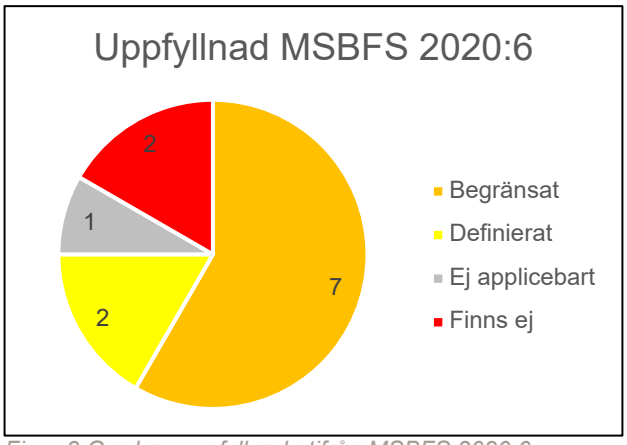
Tidigare års rapportering har baserats på ett antal områden som har relevans för området men som är svåra att mäta och följa upp. Att mäta på samma mål år efter år skapar statistik och trender vilken hjälper regionen att identifiera områden som behöver mer fokus. Då det åligger en informationssäkerhetsfunktion att sammanfatta arbetet utifrån arbetet som gjorts mot målbilden som beslutats av regionstyrelsen kommer den nya rapporteringen att utgå från de fem målområdena som specificeras i region Jämtland Härjedalens informationssäkerhetspolicy:

Figur 2 Nyckeltal (KPI) ur informationssäkerhetspolicyn

3. Måluppfyllnad 2023

3.1 Ledningssystem för informationssäkerhet (LIS)

Detta nyckeltal mäts utifrån MSB:s metodstöd för ett strukturerat informationssäkerhetsarbete och föreskriftens MSBFS 2020:6. Denna föreskrift har tolv områden som täcker in organisatoriska krav, dvs förutsättningarna för ett ledningssystem.



Figur 3 Grad av uppfyllnad utifrån MSBFS 2020:6

Status	Innebörd
Okänt	Har ännu inte undersökts
Finns ej	Helt avsaknad av styrning, processer, rutiner, etcetera
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 regionens verksamhet

Fortsatt arbete under 2024
En omfattande översyn av existerande ledningssystem för informationssäkerhet har påbörjats. Ny informationssäkerhetspolicy är ute för godkännande. En ny riktlinje för informationssäkerhet är ute på remiss som utkast och efterföljande nivåer med regler har identifierats och påbörjats.

Detta arbete tillsammans med att fastställa roller och ansvar, förslag på resurser som när stöd och ett förslag på verktygsstöd (GRC-Governance, Risk & Compliance) kommer att ge ledningssystemet en röd tråd där det blir enkelt för verksamheten att arbeta strukturerat med informationssäkerhetsfrågor.

3.2 Riskhantering

Region Jämtland Härjedalen har idag ingen enhetlig metod för riskhantering. Det har identifierats ett antal rutinbeskrivningar som används i olika grad av olika delar av verksamheten vilket innebär att det är svårt att få en överblick och status över regionens risker samt hanteringen av dessa.

Region bör ta fram en enhetlig metod för riskhantering i likhet med Region Väster Norrland med ett verktygsstöd där risker tillses en ägare, uppföljning och där ledningen kan ta strategiska beslut utifrån den samlade riskbild som är föremål för beslut.

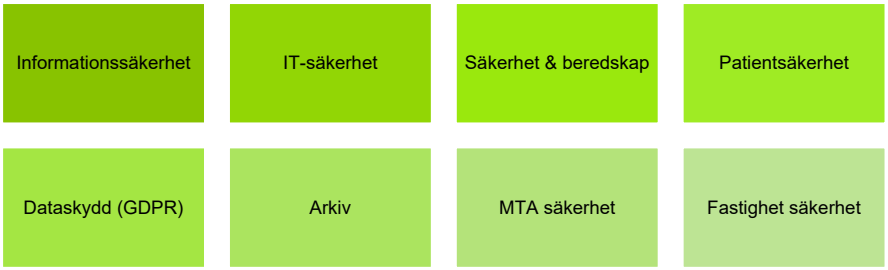
Framtida rapportering kommer att baseras på:

- Mognadsnivå – Infosäk kollen (MSB)
- Sammanfattning av övergripande riskanalys utifrån omvärldsbevakning
- % av genomförda riskanalyser utifrån identifierade verksamhetskritiska områden
- Sammanfattning av informationssäkerhetsrisker ur riskregistret utifrån riskernas nivå

Fortsatt arbete under 2024
Här genomförs det fortlöpande arbete för att samordna säkerhetsfunktionerna, införa en enhetlig metod för riskhantering med ett verktygsstöd som är ändamålsenligt för regionen och dess verksamhet.

3.3 Informationssäkerhetsorganisation

Region Jämtland Härjedalens informationssäkerhetsorganisation är idag decentraliserad utan ett tydligt ledarskap. Rollen informationssäkerhetssamordnare har ingen tydlig rollbeskrivning eller mandat gentemot de övriga funktionerna. Mycket av arbetet sker i stuprör utan insyn och med minimal samverkan.



Figur 4 Nuvarande decentraliserad säkerhetsorganisation

För att Region Jämtland Härjedalen ska kunna uppfylla sitt uppdrag och skydda dess medborgare bör säkerhetsfunktionerna arbeta mer samordnat och se säkerhetsarbetet som en helhet där de olika funktionerna tar stöd av varandra. En virtuell organisation där ansvaret mellan de olika funktionerna kartläggs och där man arbetar gemensamt med överlappande ansvarsområden.

Framtida rapportering kommer att baseras på:

Tillsatta roller och resurser/mandat för informationssäkerhetsorganisationen

Fortsatt arbete under 2024
Som en del av Ledningssystemet för informationssäkerhet måste roller och ansvar identifieras och dokumenteras. Fokus för informationssäkerhetsfunktionen kommer att ligga i att:

- Omvandla rollen informationssäkerhetssamordnaren till informationssäkerhetsansvarig (CISO)
- Med information i fokus se över och besluta om samarbete, ansvar och struktur för säkerhetsorganisationen
- Använda dagens registerkoordinatorer som informationssäkerhetssamordnare ute i verksamheten, så kallade verksamhetsnära stöd. Även detta arbete bör samverka med övriga säkerhetsfunktioner som har liknande behov.

3.4 Informationsklassning

En stor del av ett strukturerat informationssäkerhetsarbete handlar om att kartlägga och värdera (klassa) region Jämtland Härjedalens informationstillgångar. Då man än inte arbetar processbaserat på regionen har tidigare arbete utgått från informationssystem vilket även kommer att vara fokus för det fortsatta arbetet.

En förutsättning för att informationsklassa våra informationssystem och tjänster är att dessa är identifierade och dokumenterade. IT har idag över 700 identifierade system, eller IKT (Informations- och Kommunikationsteknologi). Dock finns ett stort mörkertal med hur många faktiska informationssystem regionen använder, framför allt vilka molntjänster som används.

Mörkertalet med hur många system som bör klassas tillsammans med att det inte dokumenterats vilka system som faktiskt genomgått informationsklassningar gör att det inte går att få tillförlitliga mätdata i skrivande stund.

Fortsatt arbete under 2024
Fokus kommer att ligga på att identifiera vilka informationssystem som regionen använder sig av, vilken information dessa informationssystem hanterar samt hur verksamheten har värderat informationen i de fall detta blivit gjort. Detta förutsätter att IT kan tillhandahålla en tillförlitlig databas över regionens informationssystem tillsammans med verksamhetens klassningsinformation.

En annan förutsättning är att vi tar fram en enkel klassningsmetodik, baserad på ett systemstöd (GRC) vilket kommer möjliggöra för verksamheten att efterleva gällande krav med minimal resursanvändning.

Framtida rapportering kommer att baseras på ekvationen:

% av genomförda klassningar på antal aktuella informationssystem

3.5 Informationssäkerhetsutbildning

En del av att bygga en stark informationssäkerhetskultur som i sin tur skapar en motståndskraftig organisation handlar om kvalitativ och regelbunden utbildning av alla medarbetare.

Idag genomförs en lång (45 min) och inte alltid aktuell utbildning vid anställning av medarbetare. Timanställda och konsulter är exkluderade vilket innebär att dessa grupper av medarbetare inte får någon utbildning inom informationssäkerhet fastän dessa ofta hanterar lika känslig information som ”anställda”.

Dagens uppfyllnad är 47,8% vilket är statistik från alla som genomgått utbildningen sedan den skapades för 5 år sedan. Då vi inte vet hur många av dessa personer som fortfarande arbetar kvar på regionen samt att statistiken inte går att re-producera innebär att detta inte är ett tillförlitligt mätvärde.

Fortsatt arbete under 2024
Informationsförvaltningsenheten har köpt in en färdig mikroutbildning inom informationssäkerhet som kommer att användas från hösten 2024.

Mikroutbildningen löper under 3 månader med där varje medarbetare får ett email veckovis med en länk till en delmodul som tar mellan 3–5 minuter att genomföra.

Denna mikroutbildning följer rekommendationerna inom evidensbaserad utbildning, integreras i det LMS (Learning Management System) som regionen redan använder sig av idag och är billigare än att i egen regi ta fram en ny och aktualiserad utbildning.

Ytterligare fördelar är att vi direkt kan mäta medarbetarnas genomförande av utbildningen och få tillförlitliga data över tid för att säkerställa att utbildningen kommer alla medarbetare till godo.

4 Slutsats

Mycket finns redan på plats inom informationssäkerhetsområdet även om det historiska arvet med att arbeta i så kallade stuprör har mynnat ut i att vi inte arbetar särskilt effektivt eller likartat inom området.
Stor fokus fram kommer att ligga på samverkan mellan de olika funktionerna som har ett säkerhetsansvar och att försöka ta rollen som ledare för informationssäkerhetsarbetet på region Jämtland Härjedalen. Detta kommer att vara förutsättningar för att tillsammans hitta bästa formerna för ett strukturerat arbete i enlighet med bästa praxis för både lagefterlevnad men även för att vara en betrodd leverantör för våra medborgare.