IT-stöd för informationssäkerhetsanalys i Region Sörmland

2021-04-14

Region Sörmland

Lite om oss

Vem är jag

Ann-Mari Nilsson
Informationssäkerhetsenheten Region Sörmland

Har tidigare jobbat med informationssäkerhet på IKEA, Nyköpings kommun och Migrationsverket

Vad gör Informationssäkerhetsenheten

Två medarbetare
Ger stöd och råd gällande informationssäkerhet

REGION SÖRMLAND

Informationssäkerhet

Informationstillgångar

Information (kunskap eller data) eller resurs(bärare) som hanterar information som har ett värde för Regionen.

Informationssäkerhet

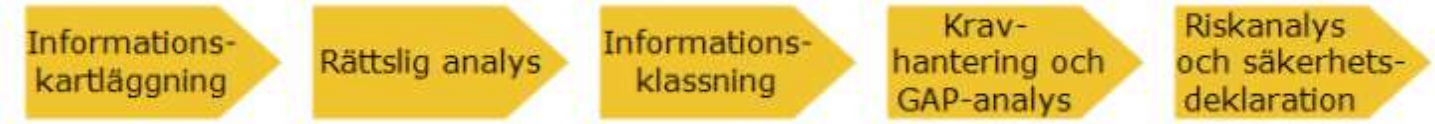
Informationssäkerhet innebär att hantera information så att

- Endast behöriga personer får ta del av den
- Den alltid går att lita på, att den är korrekt och inte är manipulerad eller förstörd
- Den alltid finns åtkomlig och användbar när den behövs

Hur säkerställs att informationen är tillräckligt säker när det finns både lagar, riktlinjer och standarder med många och olika krav på informationshanteringen?

REGION SÖRMLAND

Process för informationssäkerhetsanalys



Processen för informationssäkerhetsanalys ser till att säkerheten för regionens tillgångar omhändertas på ett enhetligt sätt.

Processen är en stödprocess.

Se till att rätt kompetenser deltar. Glöm inte bort verksamhetsspecialisterna

Informationstillgångarna är oftast objekt (IT-stöd och dess information) i förvaltning och genomförs av förvaltningen.

REGION SÖRMLAND

IT-stöd för Informationssäkerhetsanalys

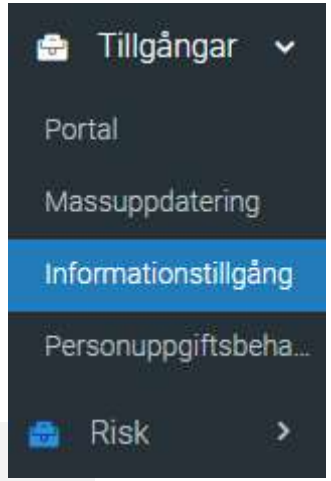
ISMS står för Information Security Management System

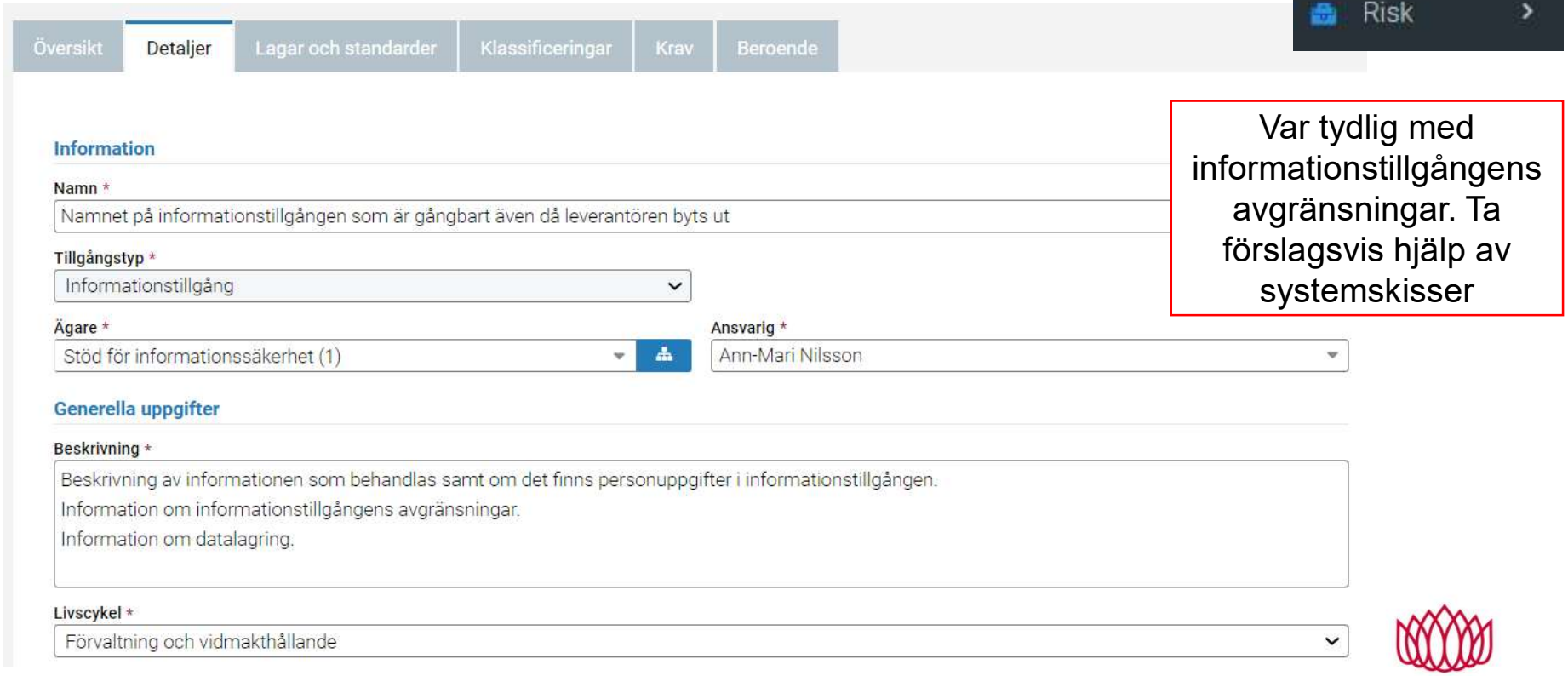
ISMS ger stöd i att:

- Följa tillämpliga lagar
- Ta fram krav på information
- Reducera risker
- Ta fram rapporter
- Att ta fram informationssäkerhetsanalyser sker på ett enhetligt sätt och analyserna lagras på ett samlat ställe med möjlighet att överblicka hela regionens informationssäkerhetsläge.

REGION SÖRMLAND

Kartläggning av information

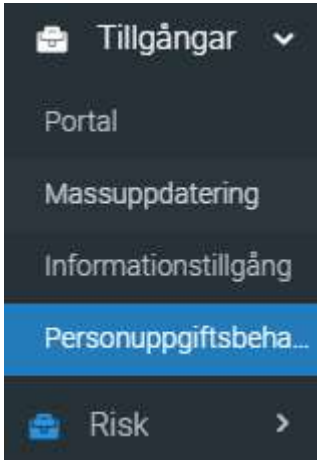




Var tydlig med informationstillgångens avgränsningar. Ta förslagsvis hjälp av systemskisser

REGION SÖRMLAND

Förteckning av personuppgiftsbehandlingar



Översikt | Detaljer | Lagar och standarder | Klassificeringar | Krav | Beroende

Information | Personuppgiftsbiträde

Information

Namn *
Administratörer av ett IT stöd eller t.ex. patientuppgifter i ett journalsystem

Tillgångstyp *
Personuppgiftsbehandling

Ägare *
Stöd för informationssäkerhet (1)

Ansvarig *
Ann-Mari Nilsson

Registerförteckning personuppgiftsbehandling

Personuppgiftsansvarig nämnd/styrelse *
Regionstyrelsen

Dataskyddsombud *
Namnet på Regionens dataskyddsombud

Behandlingens syfte/ändamål *
Om det handlar om administratörer kan det vara att lägga upp nya användare.
Om det avser Patienter kan det vara att utreda en sjukdomsbild.
Det kan också vara att informera elever, vårdnadshavare eller att bedriva skolmatsservering.

Vilken laglig grund för behandling används? *
Uppgift av allmänt intresse eller myndighetsutövning ✖
Rättslig förpliktelse ✖ | Avtal ✖ | Samtycke ✖

Vilka kategorier av registrerade? *
Invånare ✖ | Patienter ✖ | Medarbetare ✖ | Kunder ✖

Vilka kategorier av personuppgifter behandlas? *
Personnummer ✖ | Hälsouppgifter ✖

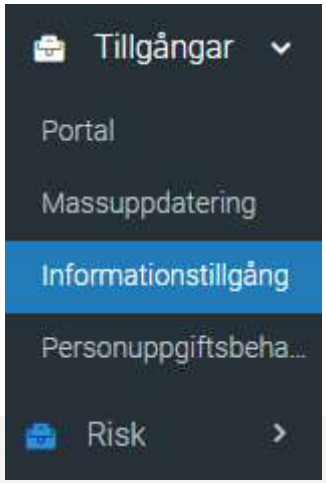
Vilka kategorier av mottagare? *
Andra myndigheter ✖

Varifrån hämtas personuppgifterna *
SCB, Eks, SPAR etc.

Krav på dataskydd enligt dataskydds-förordningen

Region Sörmland

Rättslig analys

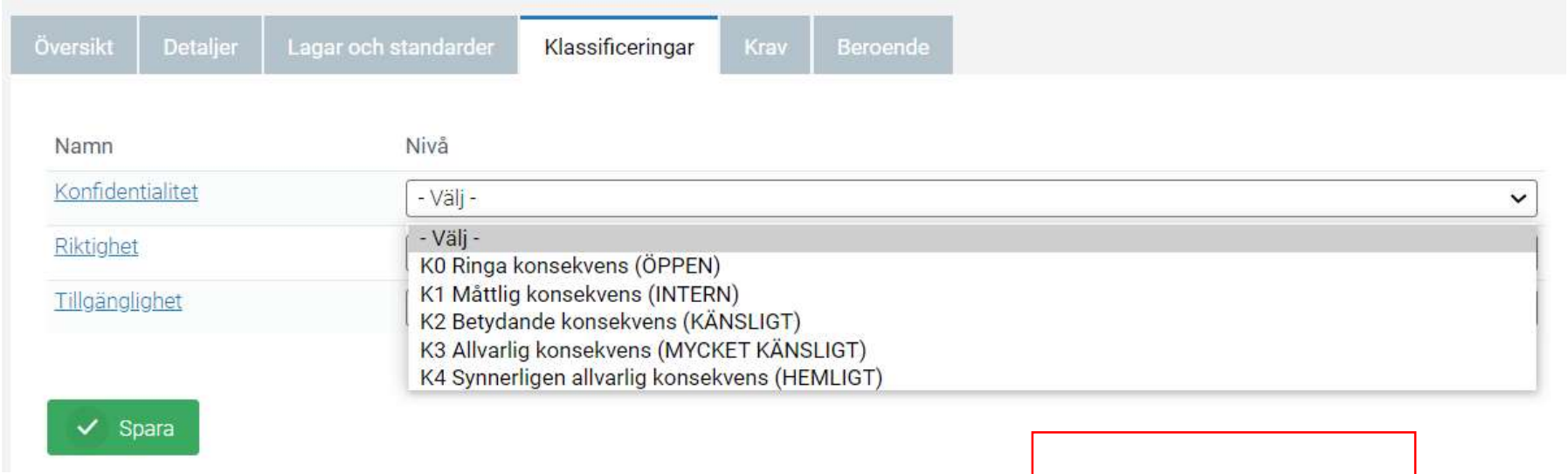


Översikt | Detaljer | **Lagar och standarder** | Klassificeringar | Krav | Beroende

Namn	Nivå
Finns det information som direkt eller indirekt kan identifiera en levande person?	Ja
Är Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster tillämplig?	Nej
Hanteras personuppgifter i syfte att bedriva vård eller tandvård	Nej
Förekommer skyddade personuppgifter?	Nej
Förekommer information som skulle hunna hota Sveriges säkerhet?	Ja
Förekommer information som används för att förebygga eller beivra brott?	Nej
Är Lag (1993:584) om medicintekniska produkter tillämplig?	Nej
Är Lag (2018:597) om kommunal bokföring och redovisning tillämplig?	Ja

Region Sörmland

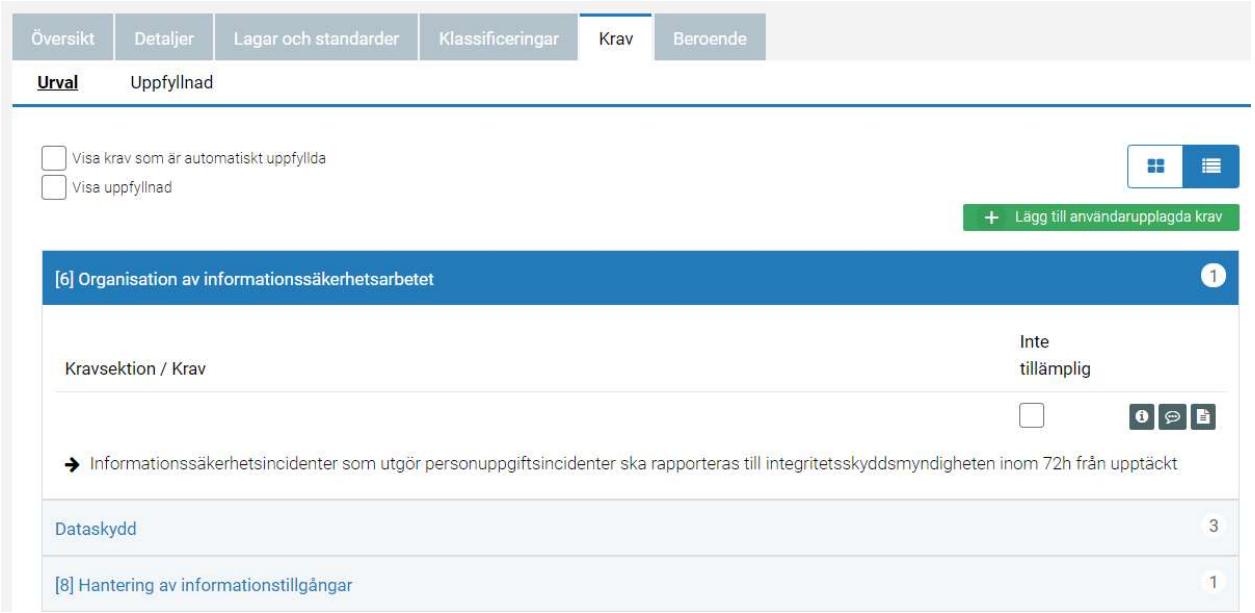
Informationsklassning



Klassa informationen utifrån sammanhang

Region Sörmland

Kravhantering och GAP-analys

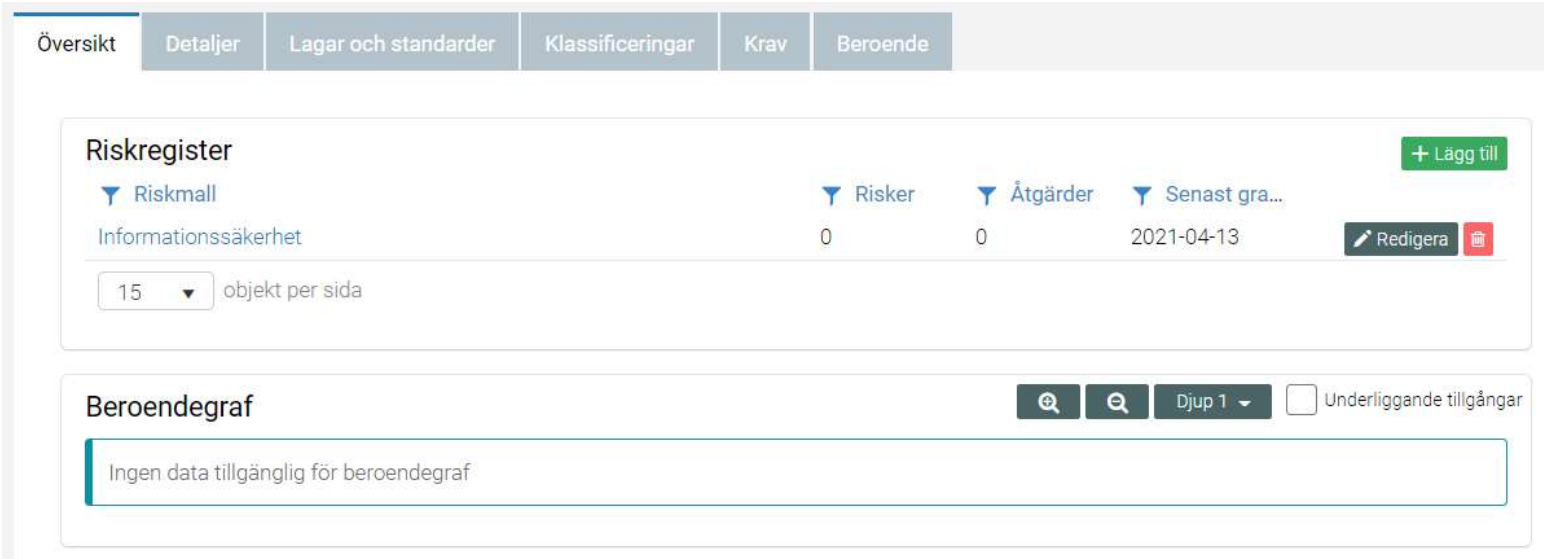


Kraven är hämtade från de åtgärder som finns definierade i ISO27002

Omhänderta GAP i riskanalysen

Region Sörmland

Riskanalys



Att identifiera risker innebär att undvika eller reducera risker genom att titta i Kristallkulan. Att vara steget före.

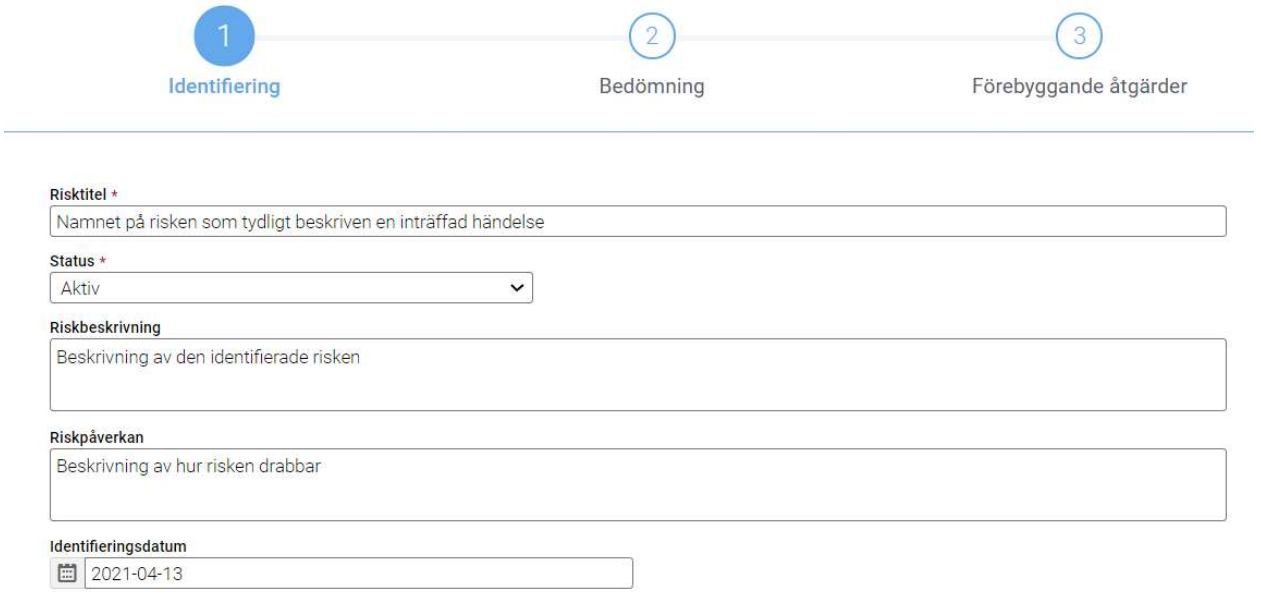
Region Sörmland

Riskregister

Vilka är hoten
Vilka är sårbarheterna
Vad är **skyddsvärdet**
Ta hjälp av tidigare inträffade händelser

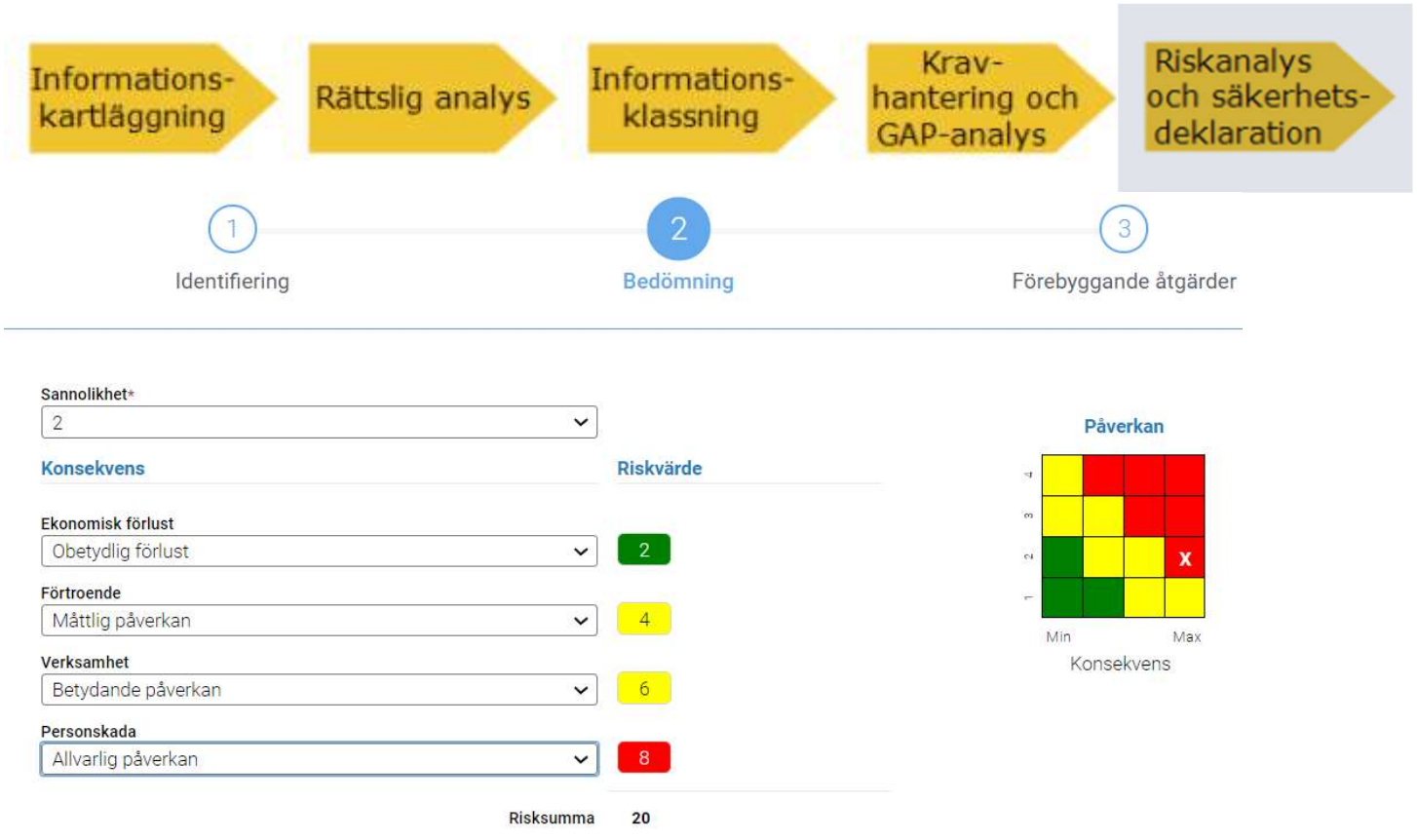
Region Sörmland

Identifiering av risk



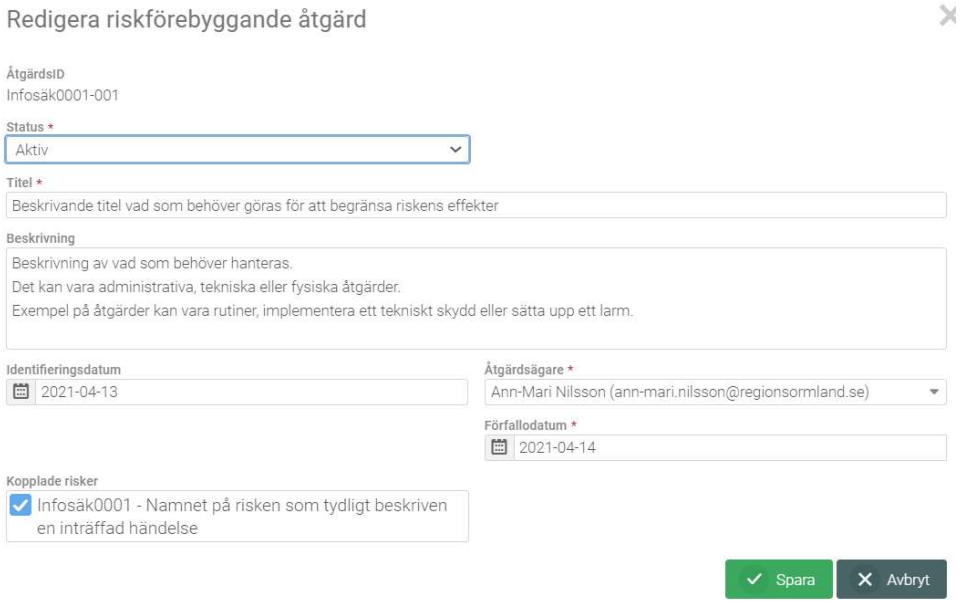
REGION SÖRMLAND

Bedömning av risk



REGION SÖRMLAND

Riskåtgärder



En risk kan ha flera åtgärder och en åtgärd kan reducera flera risker

En identifierad risk kan ge upphov till nya krav

Region Sörmland

Säkerhetsdeklaration

Säkerhetsdeklarationen ger en samlad bild av informationstillgångens skydd.

Säkerställ åtgärder och efterlevnad med

- Avtal
- Internrevision
- Externrevison

REGION SÖRMLAND

När är arbetet klar

Det är när analysen är klar som arbetet börjar

- Omhändertagandet av riskerna
- Den iterativa processen

Informationssäkerhet är aldrig starkare än dess svagaste länk, fastna inte i detaljer, plocka dem lågt hängande frukterna.

Det är bättre att färdigställa en analys än att genomföra halva processen detaljerat.

IT-stöd för informationssäkerhetsanalys

En samlad plats för samtliga informationssäkerhetsanalyser ger oss en överblick av Regionens samlade säkerhetsläge.

Ger underlag för var vi behöver ge mer stöd.

Ger uppföljning och statistik att ta med till högsta ledningens årliga säkerhetsgenomgång.

REGION SÖRMLAND