Systematiskt informationssäkerhetsarbete

Så mycket mer – och mindre – än MSB:s metodstöd.

Elina Lyckeborg och Hanna Lagerquist

Myndigheten för samhällsskydd och beredskap

Agenda

- Utgångspunkter för systematiskt informationssäkerhetsarbete
- Framtidsspaning: Hemarbete även efter pandemin?
- Avslutning och frågor

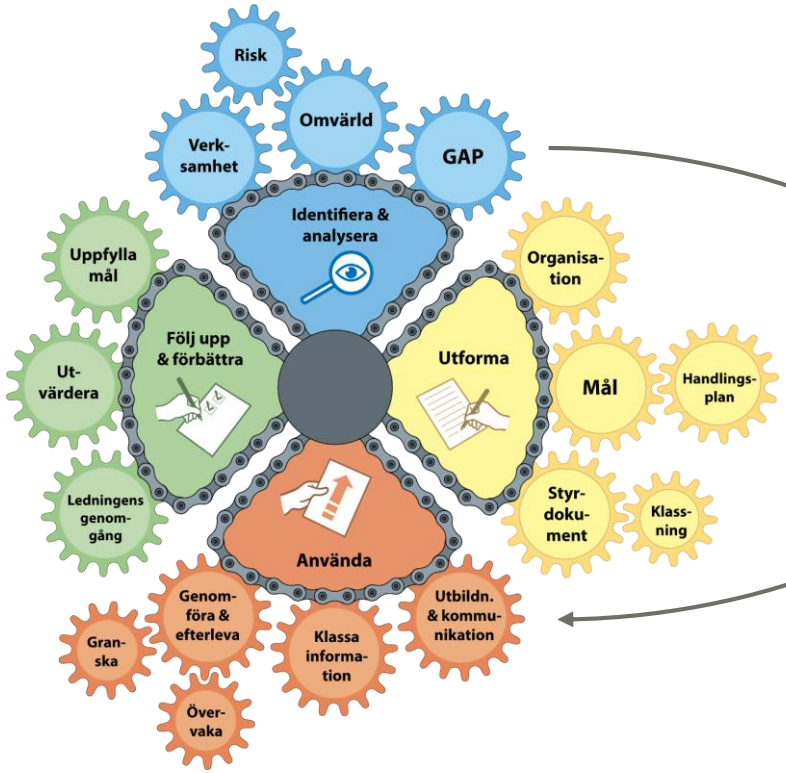
Informationssäkerheten är verksamhetens ansvar

Myndigheten för samhällsskydd och beredskap

Informationssäkerhet är verksamhetens ansvar

- Utgångspunkt: att verksamheten ska fungera
- Alla verksamheter är beroende av information och en fungerande informationshantering för att fungera
- CISO:s jobb är att hjälpa organisationen ta vara på sin information
- Begreppet CISO använder vi synonymt med begreppet informationssäkerhetssamordnare

Hur uppstår informationssäkerhet?



Myndigheten för samhällsskydd och beredskap

Hur uppstår informationssäkerhet?

- Å ena sidan finns det en verksamhet med behov av information
- Å andra sidan finns det en metod för systematiskt informationssäkerhetsarbete, som inte kan passa alla organisationer
- CISO är bryggan mellan dessa, som anpassar metoden för den specifika organisationen och stöttar verksamheterna i att skydda informationen

Vad kan du begära av verksamheten?

Vilken information de har som är viktig och varför

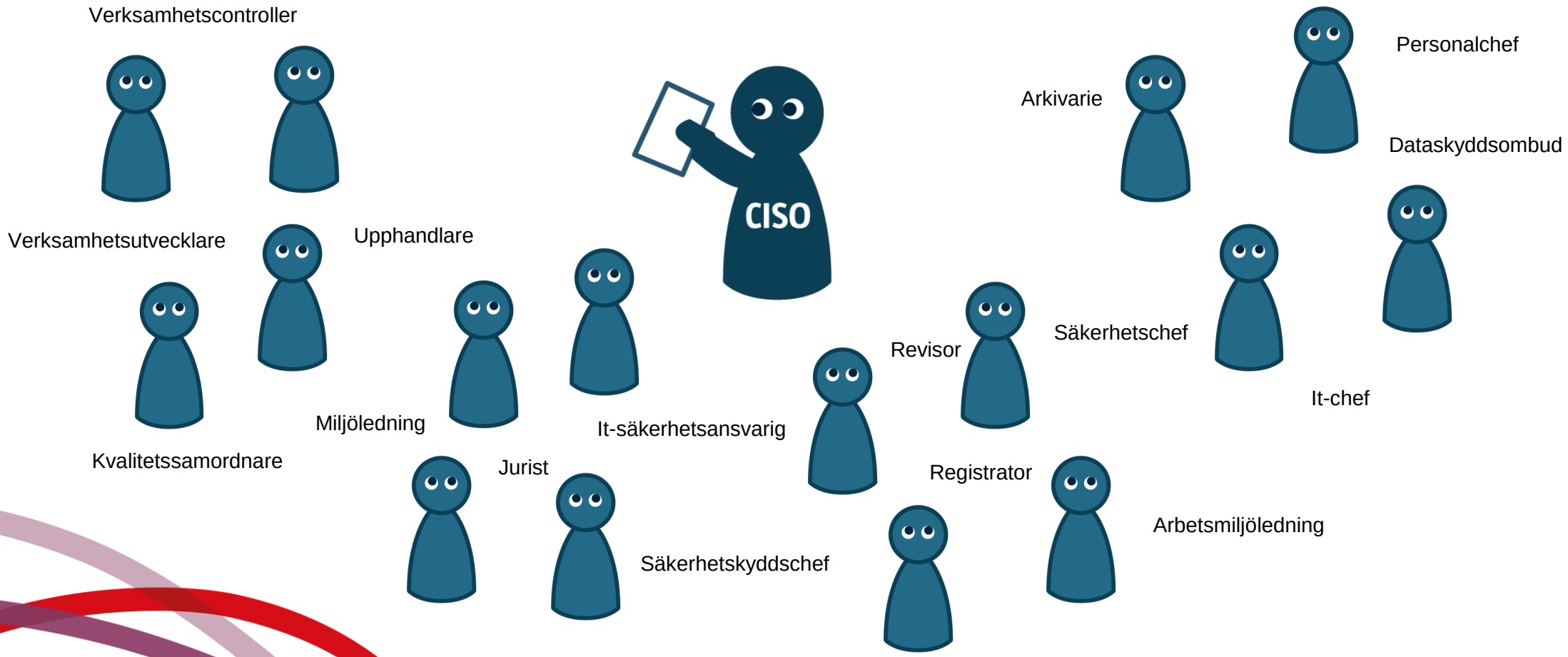
Fattar beslut och tilldelar medel

Agerar på ett informationssäkert sätt

Sammanfattningsvis

- Informationssäkerheten är verksamhetens ansvar
- CISO:s uppgift är att hjälpa verksamheten att ta sitt ansvar

CISO:s vänner
Nyckelroller i informationssäkerhetsarbetet



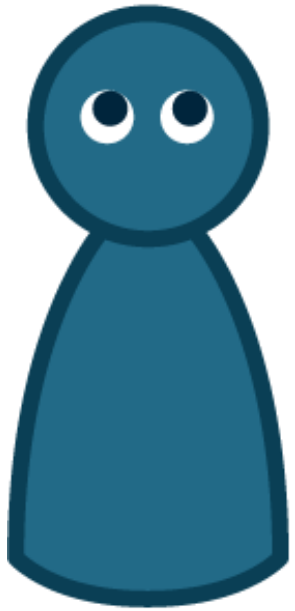
Myndigheten för samhällsskydd och beredskap

Juristen

Styrdokument

Kan strukturen

Kan formulera



Vill att alla ska förstå och kunna följa

Efterlevnad är viktigt

Hittar rättsliga hinder

Kan organisationen

Kan beredningss- och beslutsgångar

Juristen

Får hjälp att formulera och implementera styrdokument

Får hjälp att navigera beredningss- och beslutsgångar

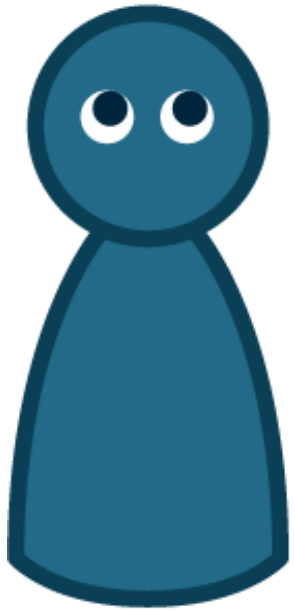
Myndigheten för samhällsskydd och beredskap

Verksamhetscontrollern

Skapar strukturer

Ordning och reda

Följer upp verksamhetsrisker



Metodstöd för riskanalys

Håller reda på årshjul

Myndigheten för samhällsskydd och beredskap

Verksamhetscontrollern

Får hjälp att följa årshjulet

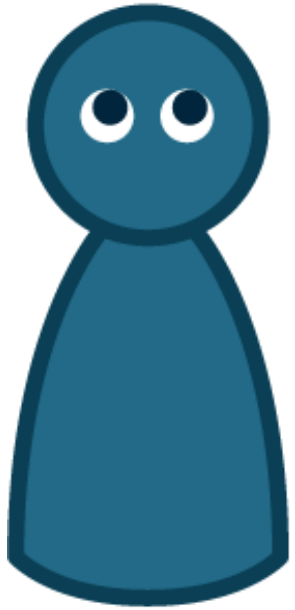
Får hjälp att anpassa riskanalysarbetet

Myndigheten för samhällsskydd och beredskap

Upphandlaren

Koll på upphandlings-processen

Stöttar verksamheten i upphandlingar



Van att formulera krav

Äger styrdokument som rör upphandling

Myndigheten för samhällsskydd och beredskap

Upphandlaren

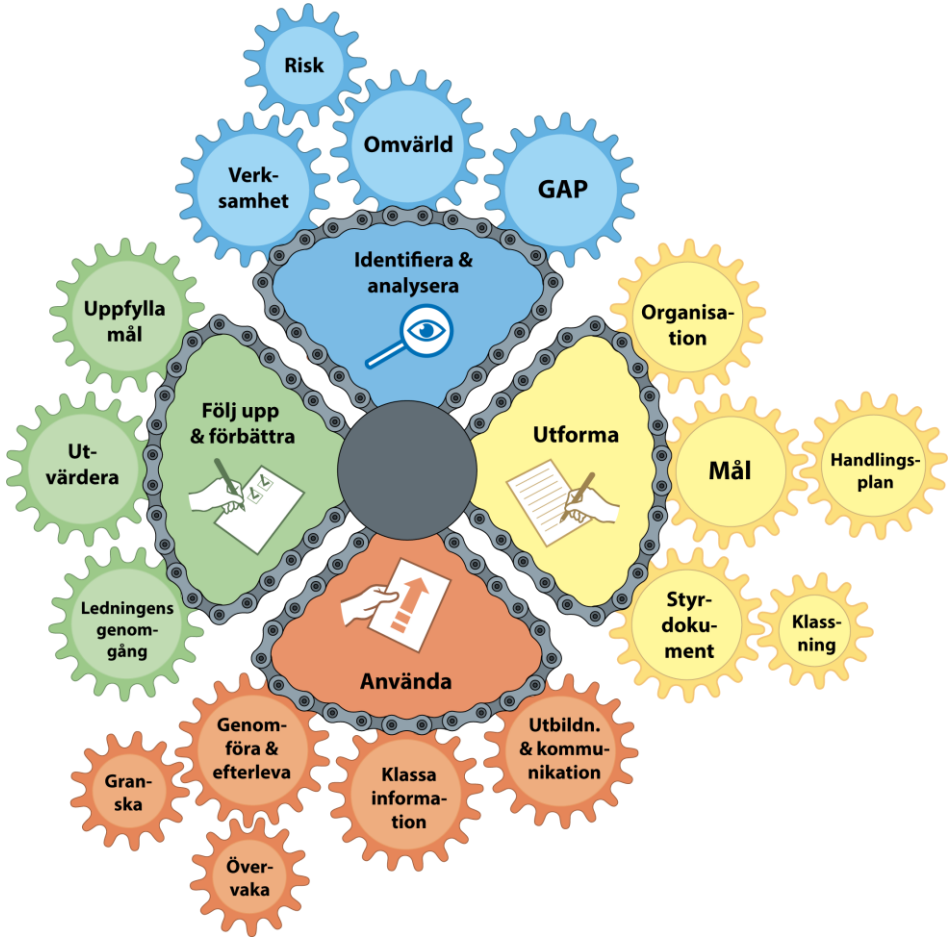
Får hjälp att stötta verksamheten i kravställning

Får hjälp att föra in informationssäkerhet i upphandlings-processen

Sammanfattningsvis

- Det finns många andra roller som har till uppgift att ta hand om sådant som är relaterat till informationssäkerhetsarbetet
- Ta hjälp av varandra – både ditt och andras jobb blir lättare
- Läs mer om CISO:s vänner i Nyckelroller i informationssäkerhetsarbetet i Metodstödet

Man kan börja var som helst



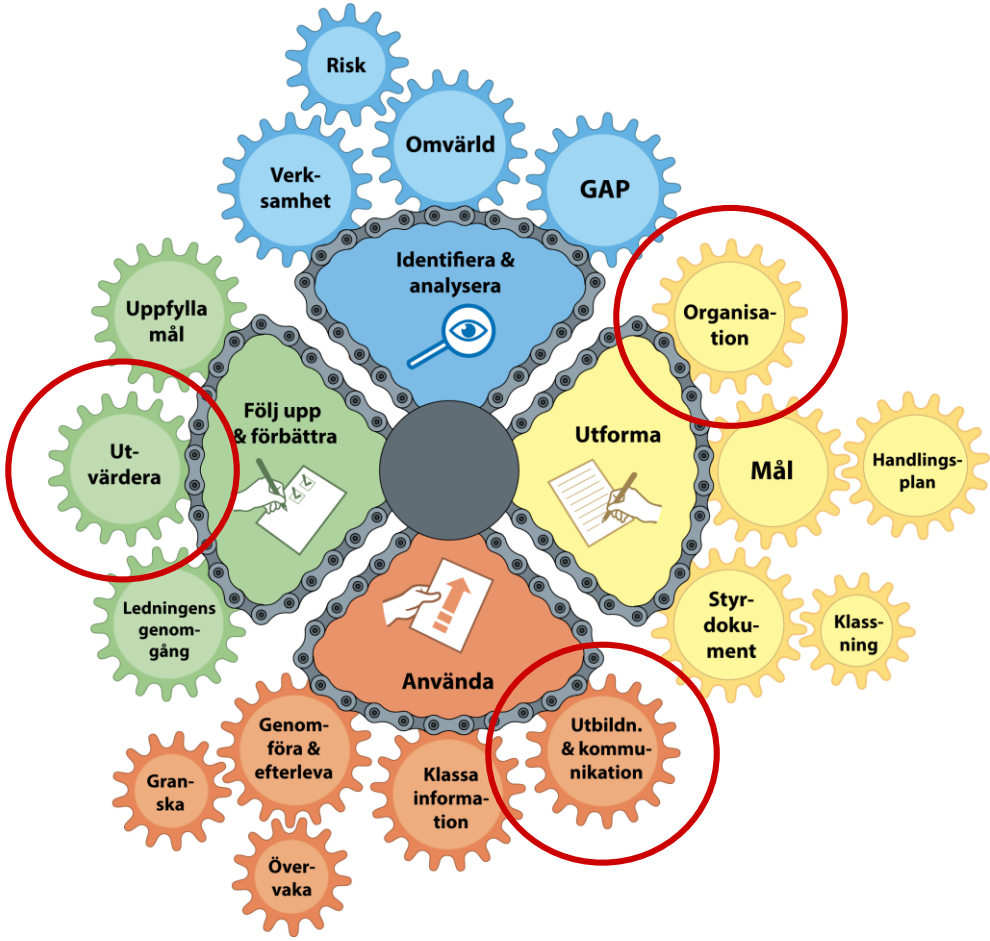
Myndigheten för samhällsskydd och beredskap

Vad avgör var jag börjar?

- Där det finns störst risk
- Där det redan pågår ett arbete
- Där du får gehör

Man kan börja var som helst

Till exempel i…



Myndigheten för samhällsskydd och beredskap

Utbilda ledningen

- Varför, vad, hur
- Din syn
- Ert samarbete

Berätta om ditt uppdrag

- Internkommunikation
- Bjud in dig själv
- Vad du vet och var du börjar

Utbilda medarbetare

- Förmedla utbildningar från MSB
- Skapa en egen utbildning

Utbilda ledningen

Lär ut vad du kan

- Varför är informationssäkerhet viktigt
- Vad är informationssäkerhet
- Hur fungerar informationssäkerhet
- Hur ser du på informationssäkerhet
- Hur arbetar en ledning och CISO tillsammans

Berätta om ditt uppdrag

Du har fått ett uppdrag att ”göra något med informationssäkerhet”

- Ta kontakt med internkommunikation – hur når man ut i organisationen
- Bjud in dig själv till större sammankomster/möten
- Presentera dig och något om vad du ska jobba med
- Håll det enkelt, berätta vad du vet och var du börjar

Utbilda medarbetare

Utgå från din känsla av vad som behövs

- DISA eller motsvarande till alla
- Informationssäkerhet för ansvarsroller
- Knåpa ihop en enkel utbildning som tar upp relevanta områden och innehåller länkar till den stöd och hjälp som finns (oavsett hur mycket som finns)

Lämplighet, tillräcklighet och verkan

- Identifiera den styrning som redan finns
- Gör en bedömning om styrningen är lämplig, tillräcklig och verkningsfull

Övervakning och nyckeltal

- Hör med ansvariga vilken loggning/ driftövervakning som finns
- Hör med verksamhetscontrollern om styrningsuppföljning och resultat
- Om LIS finns – följ upp efterlevnad

Mognadsanalys eller benchmarking

- Går att köpa in mognadsanalys eller göra själv
- Gå med i nätverk och hitta liknande organisationer som kan dela med sig

Följ upp lämplighet, tillräcklighet och verkan

- Identifiera den styrning som redan finns
- Gör en bedömning om styrningen är
  - Lämplig – står styrningen i samklang med organisationens övergripande mål?
  - Tillräcklig – leder styrningen till en risknivå som överensstämmer med ledningens riskaptit?
  - Verkningsfull – efterlevs styrningen, finns säkerhetsåtgärderna på plats och fungerar?

Inventera och följ upp övervakning och nyckeltal

- Vad loggas och mäts idag i organisationen – och i vilket syfte? Räcker detta eller borde fler saker loggas?
- Vilka nyckeltal finns? Vad används de till?
- Vilka nyckeltal borde finnas för informationssäkerhetsarbetet?

Genomför mognadsanalys eller benchmarking

- Mät informationssäkerhetsmognad eller ledningssystemets övergripande mognad
- Nätverk finns hos MSB och i en mängd mindre konstellationer som bygger på förtroende

Ingångsvärden

- Organisationsstruktur
- Namn på roller och ansvarsområden
- Mandat och budgetområden

Ansvar för informations-säkerhet

- Koppla till roller som finns i organisationen
- Mandat att hantera risk
- Ansvar för informationssäkerhet

Ansvar för informations-säkerhetsarbetet

- Mandat
- Ansvar för informations-säkerhetsarbetet

Ingångsvärden

- Interna dokument
  - organisationsbeskrivningar
  - befattningsbeskrivningar
  - styrdokument
  - arbetsordning
  - delegationsbeslut
- Eftertraktat innehåll
  - Organisationsstruktur
  - Namn på roller och ansvarsområden
  - Mandat och budgetområden

Ansvar för informationssäkerhet

Utgångspunkt: Följer verksamhetsansvaret

- Koppla till roller som finns i organisationen
- Specificera mandat att hantera risk
  - Mandat att hantera risk som enbart påverkar eget ansvarsområde samt ryms inom egen budget.
- Specificera ansvar för informationssäkerhet
  - Ansvar att eskalera hantering av risk som påverkar utanför eget ansvarsområde eller inte ryms inom budget.
  - Tips! Kika på ansvarsförklaringar från andra områden, såsom miljö, arbetsmiljö, kvalitet m.m.

Ansvar för informationssäkerhetsarbetet

CISO:s roll

- Specificera mandat
  - Mandat att besluta vad som ska rapporteras samt rapportera till högsta ledningen.
  - Mandat att skapa beslutsunderlag för högsta ledningen
  - Mandat att leda och fördela arbetet för ev. dedikerade resurser.
- Specificera ansvar informationssäkerhetsarbetet
  - Ansvar att skapa, förvalta och till organisationen tillhandahålla nödvändiga
    - Modeller
    - Metoder
    - Stöd

Sammanställ resultat och få beslut

- Dokumentera resultatet i ett eller flera styrdokument enligt organisationens struktur för styrdokument.
- Föredra för högsta ledningen, var beredd på frågor.
- Begär beslut.

Sammanfattningsvis

- Det är inte meningen att man ska göra allt på en gång
- Hitta det minsta du kan göra som blir ett underlag till nästa steg – oavsett om nästa steg är att begära mer resurser från ledningen, göra en analys, eller skapa ett styrdokument
- Var realistisk och transparent

Arbeta hemma…

Från undantag till ett nytt normalt?

Hitta de goda exemplen!

Myndigheten för samhällsskydd och beredskap

Tack!

Myndigheten för samhällsskydd och beredskap