

Rollbeskrivningar i Informationssäkerhetsprogram 2020

Roller inom budgetnivå

Roller inom budgetnivån ansvarar för beslut om tilldelning och förändring i resurser. Inom PM3 används begreppen Objektägare och Objektägare IT, för att förtydliga rollernas innebörd används båda benämningarna i beskrivningarna.

Informationsägare/Objektägare

Den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids. Informationsägaren är därmed riskägare för den information som ska hanteras i IT-systemet/lösningen. För att hantera risken bör informationsägaren genomföra en riskanalys. Om det finns flera informationsägare som ska använda IT-systemet/lösningen bör samtliga delta i riskanalysen.

Eftersom skadeverkningarna av bristande säkerhet i IT-systemet/lösningen uppstår hos informationsägaren är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning.

De interna relationerna mellan informationsägare och systemägare bör, när det gäller informationssäkerhet, utgå från informationsägaren.

Kan vara en förvaltningschef/verksamhetschef.

Det operativa arbetet kan utföras av en förvaltningsledare/informationsförvaltare.

Närmast jämförbara rollen enligt förvaltningsmodellen PM3 är Objektägaren som har det övergripande ansvaret för det verksamhetsnära förvaltningsarbetet inom objektet.

Systemägare/Objektägare IT

Person eller enhet som har det övergripande ansvaret för ett eller flera IT-system/lösning/komponenter. IT-systemet/lösningen/komponenten hanterar alltid en eller flera informationsmängd(er). För att hantera risker bör systemägare genomföra en riskanalys. Utifrån riskanalysen och informationsägarens krav på skydd är det systemägarens ansvar att tillse att adekvata skydd skapas.

Kan vara en förvaltningschef/verksamhetschef.

Det operativa arbetet utförs oftast av en förvaltningsledare IT.

Närmast jämförbara rollen enligt förvaltningsmodellen PM3 är objektägaren IT som ansvarar för att det finns adekvata system eller liknande som hanterar verksamhetens information. Objektägaren ansvarar för att det finns adekvat skydd för den information som lagras eller bearbetas i systemet.

Roller inom beslutsnivå

Roller inom beslutsnivån koordinerar och styr förvaltningsarbetet så att förvaltningsplanens mål uppnås med de tilldelade resurserna. Inom PM3 används begreppen Förvaltningsledare och Förvaltningsledare IT.

Informationsförvaltare/Förvaltningsledare

Informationsförvaltare är den som aktivt förvaltar informationen på informationsägarens uppdrag.

Syftet med informationsförvaltning är inte bara att bevara handlingarna och göra dem läsbara under den tid som krävs. Syftet är snarast att bevara handlingar som bevis för transaktioner så länge dessa bevis krävs eller är av värde.

Delfunktioner som ingår i informationsförvaltningen är:

- Registratur
- Dokumentation – Dokumenthantering
- Arkivering
- Arkivförvaltning
- Informationssäkerhet
- Gallring

Inom systemförvaltningsmodellen PM3 motsvaras informationsförvaltaren närmast av rollen förvaltningsledare. Förvaltningsledare finns på beslutsnivån inom den objektnära förvaltningen och leder förvaltningsarbetet samt arbetar för att säkerställa att förvaltningsplanens mål nås. Rollen förvaltningsledare motsvaras av projektledare inom projekt.

Systemförvaltare/Förvaltningsledare IT

Systemförvaltaren är den som aktivt förvaltar IT-systemet/komponenten på systemägarens uppdrag.

Arbetet är proaktivt för att upprätthålla och utveckla IT-stöd. Ett effektivt nyttjande kräver att någon prioriterar arbetet kring objektförvaltning.

Rapporterar till systemägare.

Inom systemförvaltningsmodellen PM3 motsvaras systemförvaltaren närmast av rollen förvaltningsledare IT. Förvaltningsledare IT finns på beslutsnivån inom den IT-nära förvaltningen.

Informationssäkerhet

Roller inom informationssäkerhet som inte ingår i förvaltningsmodellen PM3.

Informationssäkerhetssamordnare

Informationssäkerhetssamordnaren ska bedriva arbetet med informationssäkerhet. För att IT-stödet ska fungera så behövs ett metodiskt, systematiskt och långsiktigt informationssäkerhetsarbete.

Arbetsuppgifter som ingår i rollen kan inkludera:

- Ansvar att förvalta och utveckla ledningssystemet för informationssäkerhet.
- Genomföra risk- och sårbarhetsanalyser inom området IS/IT och informationssäkerhet.
- Genomföra interna kontroller/revisioner inom informationssäkerhetsområdet.
- Delta och representera informationssäkerhet i samverkans/styrgrupper inom informationssäkerhet och IS/IT.
- Leda och delta i lokala och regionala projekt inom informationssäkerhetsområdet samt representera informationssäkerhet i andra IS/IT relaterade projekt.

Bra kompetenser för rollen:

- Risk- och kontinuitetshandling
- Informationsteknik
- Projektledning
- Juridik
- Kommunikation

Dataskyddsombud (DPO)

Den nya dataskyddsförordningen, GDPR, ställer krav på att alla offentliga myndigheter så som kommuner, landsting och regioner ska ha ett Dataskyddsombud. Ombudet ersätter den tidigare rollen Personuppgiftsombud från Personuppgiftslagen.

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. Det innebär bland annat att:

- Samla in information om hur organisationen behandlar personuppgifter
- Kontrollera att organisationen följer bestämmelser och interna styrdokument
- Informera och ge råd inom organisationen.

Dataskyddsombudet ska också:

- Ge råd om konsekvensbedömningar
- Vara kontaktperson för Datainspektionen
- Vara kontaktperson för de registrerade och personalen inom organisationen
- Samarbeta med Datainspektionen, till exempel vid inspektioner.

Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvariga eller hos personuppgiftsbiträdet

Ombudet ska utses på grundval av yrkesmässiga kvalifikationer, besitta sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra uppgifter i linje med organisationen. Rollen får ingå i den personuppgiftsansvariges eller bitrådets personal, men dataskyddsombudet ska

inte ha andra arbetsuppgifter som kan krocka med rollen som dataskyddsbud. Rollen kan samordnas av flera kommuner om det är lämpligt utifrån uppgiftens omfattning och komplexiteten i verksamheterna. Hänsyn ska tas till om ombudet kan antas fullgöra sina uppgifter för all myndigheter och vara lika tillgänglig för de olika personuppgiftsansvariga nämnderna och för registrerade individer.

Dataskyddsbudets kontaktuppgifter ska skickas till Datainspektionen.

<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/dataskyddsbud/>

Följande bild är en illustration över de olika rollerna och samarbetet/kommunikationen vid hantering av personuppgifter:

