Malin Ekblad
Säkerhetschef
malin.ekblad@trelleborg.se

Kommunstyrelsen

Bilaga 1 – Information om riskanalys för informationssäkerhet

Nedan följer en genomgång av riskanalysens olika delar.

Informationsklassning

I riskanalysen specificeras vilken information som finns i systemet. Informationen klassificeras enligt informationssäkerhetsprinciperna *konfidentialitet, riktighet, tillgänglighet och spårbarhet* (se klassificeringsmodell ovan). Utifrån klassificeringen får systemet ett skyddsvärde på respektive informationssäkerhetsprincip. Utifrån skyddsvärdet på systemet så rekommenderas lämpliga säkerhetsåtgärder.

Skyddsåtgärder

I skyddsåtgärderna bedöms bland annat åtkomst (behörigheter, autentisering eller stark autentisering), loggning, säkerhetskopiering, Anskaffning och utveckling av system, tredjepart/leverantörer, användarens ansvar, kryptering, rutiner för avvikelsehantering, drift, personuppgifter & kommunikation och nätverk.

Riskhantering

Vidare identifieras vilka risker som finns i systemet och risken klassificeras utifrån sannolikhet att något inträffar och konsekvens för verksamheten om risken inträffar. Sannolikheten att något kan inträffa är enligt följande:

1. Mycket Sällan – en gång på 10 år
2. Sällan - En gång på 1 år
3. Regelbundet – en gång på 1 månad
4. Ofta – en gång på 1 vecka

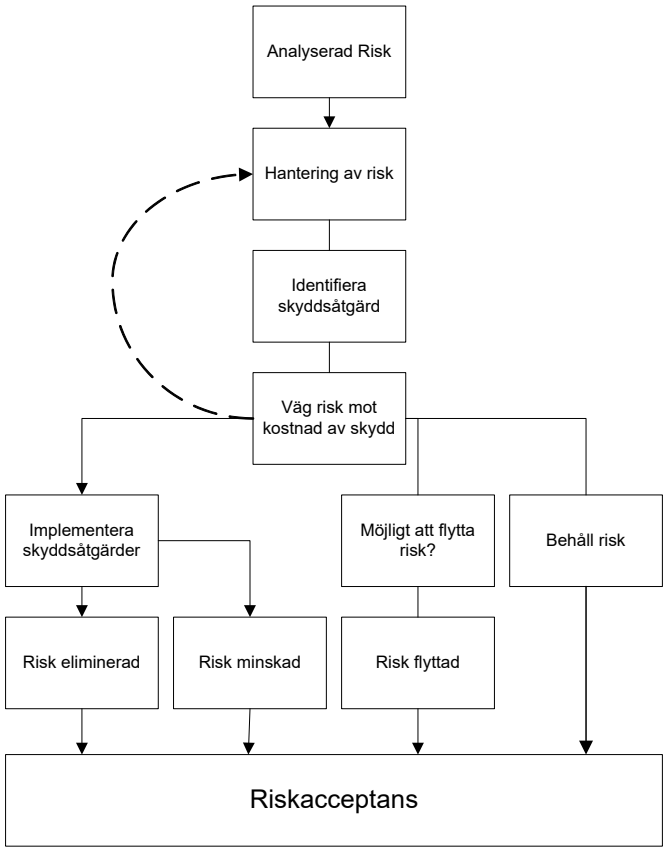
Konsekvensen är ett mått på den skada en risk skulle ha på verksamheten om den inträffar. Påverkan kan vara direkt eller indirekt, ekonomisk eller mänsklig. I modellen använder vi oss av nivåerna:

1. Försumbar – Kan innebära kostnader upp till max 10 000 kr
2. Måttlig – Kan innebära kostnader upp till max 100 000 kr
3. Betydande - Kan innebära kostnader upp till max 1 000 000 kr
4. Allvarlig - Kan innebära kostnader upp till max 30 000 000 kr

Utifrån denna klassificering får respektive risk ett riskvärde, där ett högre riskvärde innebär en högre risk.

	Mycket sällan	Sällan	Regelbundet	Ofta
Försumbar	1	2	3	4
Måttlig	2	4	6	8
Betydande	3	6	9	12
Allvarlig	4	8	12	16

Nästa steg i riskhanteringsprocessen är att hantera risker som identifierats och bedömts. En risk kan minskas, elimineras, flyttas eller accepteras. Målet är att inga risker skall accepteras utan att ett medvetet val gjorts kring detta. Bilden nedan illustrerar processen för riskhantering:



HUKI-analys

Därefter görs en HUKI-analys, som innebär att det utses en huvudansvarig för respektive risk, det utses vem som ska arbeta med risken (utförare), vem som behöver konsulteras för att arbeta med risken och vem man ska informera om vidtagna åtgärder .

Hur klarar systemet GDPR (Dataskyddsförordningen)?

Därefter kontrolleras vilka personuppgifter som hanteras i systemet, att de stämmer överens med de behandlingar som är registrerade i kommunens, bolagens registerförteckning, att biträdesavtal och sekretessavtal är skrivna samt huruvida systemet uppfyller lagkraven enligt dataskyddsförordningen (GDPR). Avslutningsvis analyseras behovet av backup för systemet (säkerhetskopiering), vilket ligger till grund för det avtal systemägaren ska ha med IT-avdelningen och/eller systemleverantören.

Rekommendation & summering

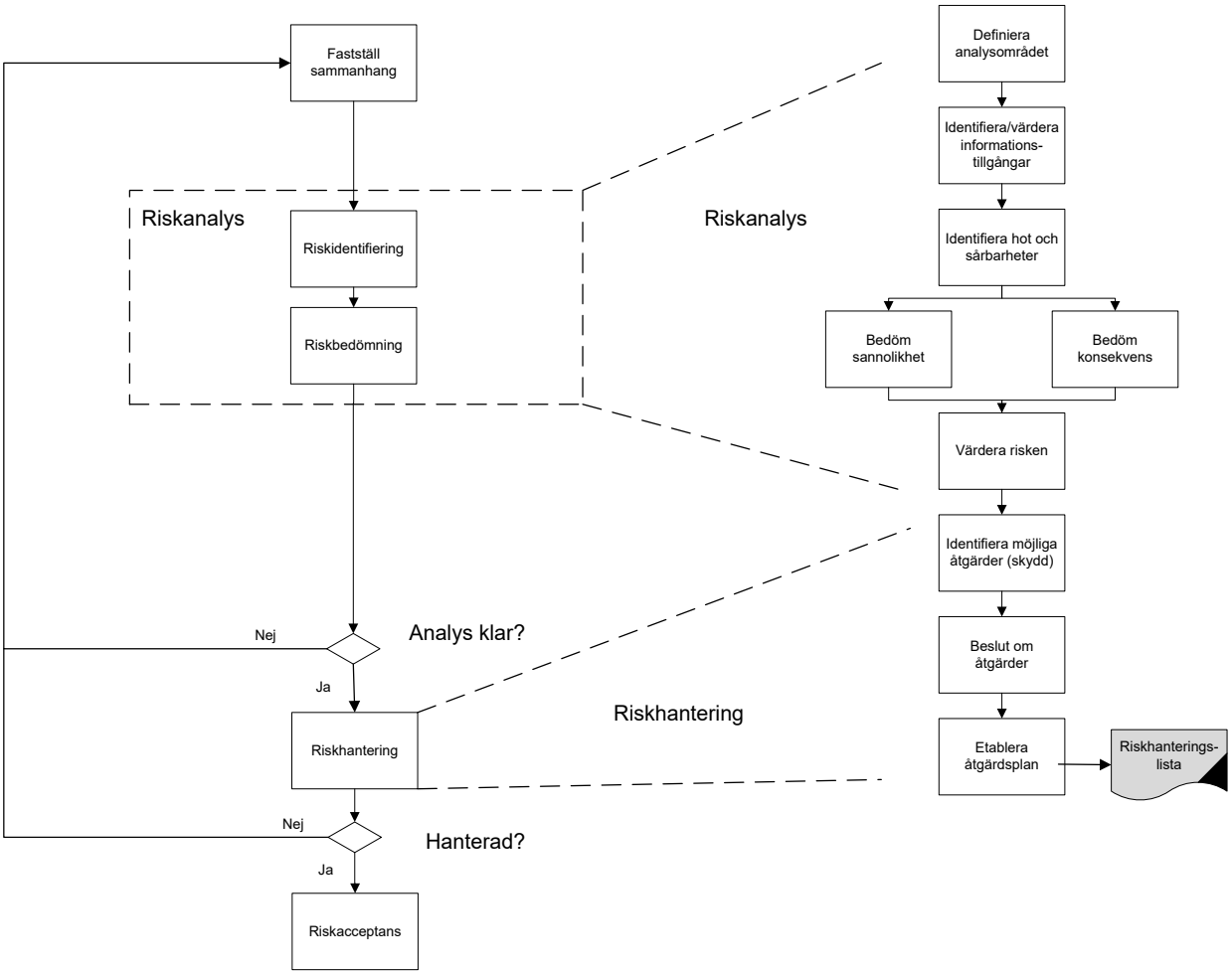
IT och informationssäkerhetssamordnaren ska vid riskanalysen lämna en rekommendation om huruvida de anser att systemet uppfyller kraven och om det bör driftsättas/får fortsatt användas inom kommunen, bolagen.

Vid negativ rekommendation ska detta informeras till ansvarig nämnd eller bolag som tar beslut om systemet ska få driftas eller inte.

Riskanalysen ska genomföras innan ett system köps in/börjar användas i kommunen. Analys ska fortlöpande göras en gång per år för samtliga system som hanterar personuppgifter eller verksamhetsinformation.

Det är systemägarens ansvar att riskanalysen genomförs och att rekommenderade åtgärder vidtas. Inledande riskanalys ska göras av systemägaren eller systemansvarig tillsammans med informationssäkerhetssamordnaren och utsedd medarbetare från IT-avdelningen.

Den årliga uppföljande riskanalysen ska vid behov göras av systemägaren eller systemansvarig tillsammans med informationssäkerhetssamordnaren och utsedd medarbetare från IT-avdelningen. Förekommer det inget behov av gemensam uppföljning kan systemägaren alternativt systemansvarig göra riskanalysen själv och informera informationssäkerhetssamordnaren samt IT-avdelningen om resultatet. Upphandling av nytt system ska ske i samråd med IT-avdelningen. Vid förändring i system, som exempelvis när ny information läggs till, ska detta rapporteras till IT-avdelningen.


Fastställ sammanhang
Riskanalys
Riskidentifiering
Riskbedömning
Definiera analysområdet
Identifiera/värdera informations-tillgångar
Identifiera hot och sårbarheter
Bedöm sannolikhet
Bedöm konsekvens
Värdera risken
Riskanalys
Identifiera möjliga åtgärder (skydd)
Beslut om åtgärder
Etablera åtgärdsplan
Riskhanterings-lista
Nej
Analys klar?
Ja
Riskhantering
Riskhantering
Nej
Hanterad?
Ja
Riskacceptans