

Metodstöd för riskhantering av information

Diarienummer: KS-2026/00250

Datum för upprättande: 2026-09-18

Innehåll

Inledning	4
------------------------	----------

Informationsklassning	6
------------------------------------	----------

Inledande information	6
-----------------------------	---

Förbered informationsklassning	8
--------------------------------------	---

1. Initiera	8
-------------------	---

2. Bestäm deltagare	8
---------------------------	---

3. Hämta underlag	9
-------------------------	---

Genomför informationsklassning	10
--------------------------------------	----

1. Inleda workshop	10
--------------------------	----

2. Definiera klassningsobjekt	10
-------------------------------------	----

3. Verksamhets- och juridisk analys	10
---	----

4. Kris- och kontinuitetsanalys	10
---------------------------------------	----

5. Klassa information	11
-----------------------------	----

Arbete efter informationsklassning	12
--	----

1. Rapportera resultat	12
------------------------------	----

2. Diarieför handlingar	12
-------------------------------	----

Analyser efter informationsklassning	13
--	----

Riskanalys och val av säkerhetsåtgärder	13
---	----

Konsekvensbedömning avseende dataskydd (DPIA)	13
---	----

Riskanalys	14
-------------------------	-----------

Inledande information	14
-----------------------------	----

Övergripande information	14
--------------------------------	----

När ska en riskanalys genomföras?	15
---	----

Metod för genomförande	15
------------------------------	----

Förbereda	15
-----------------	----

1. Utse deltagare	15
-------------------------	----

2. Hämta underlag inför riskanalys	15
--	----

Genomföra	16
-----------------	----

1. Identifiera	16
----------------------	----

2. Värdera	16
------------------	----

3. Prioritera	17
---------------------	----

Arbete efter riskanalys	18
1. Åtgärdsplan.....	18
2. Diarieför handlingar	18
Val av säkerhetsåtgärder	19
Inledande information	19
Vad är en säkerhetsåtgärd?	19
Hantering av identifierade risker	20
Välja säkerhetsåtgärder	20
Uppföljning.....	21

Inledning

Detta metodstöd är utformat för att stödja kommunens verksamheter i arbetet med riskhantering av information. Syftet är att ge vägledning i hur verksamheterna ska genomföra informationsklassningar, riskanalyser, välja lämpliga säkerhetsåtgärder och följa upp riskhanteringen. Metodstödet beskriver praktiskt hur riskhanteringsprocessen kan tillämpas och bidrar samtidigt till att hela kommunen arbetar enhetligt.

Metodstödet är utformat så att användaren kan gå till de avsnitt som är mest relevanta för det aktuella arbetet.

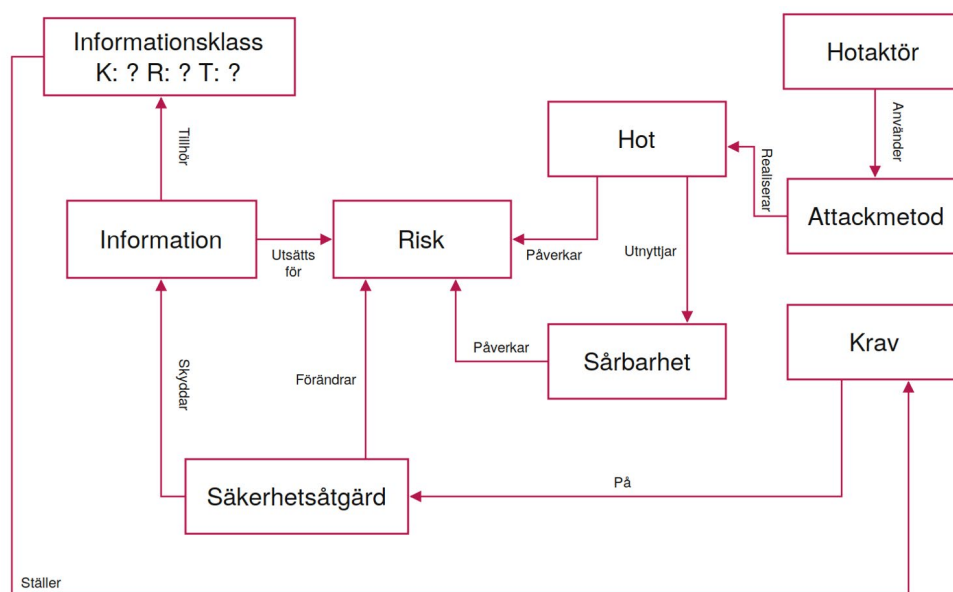
Syftet med riskhantering

Arbetet med riskhantering inkluderar informationsklassning, riskanalys, val av åtgärder och uppföljning. Syftet med riskhantering är att säkerställa att informationen skyddas i enlighet med dess betydelse för verksamheten och gällande lagstiftningar. Informationsklassning fastställer informationens skyddsbehov och ökar medarbetares medvetenhet om konsekvenserna av bristande skydd, medan riskanalyser identifierar och värderar hot och sårbarheter mot dessa tillgångar. Resultatet från informationsklassningar och riskbedömningar används som underlag för att välja ändamålsenliga och proportionerliga säkerhetsåtgärder, så att skyddet anpassas både till informationens skyddsbehov och verksamhetens aktuella risker.

Principer

Inom ramen för riskhantering utgör konfidentialitet, riktighet och tillgänglighet centrala principer för bedömning och hantering av information. **Konfidentialitet**, säkerställer att information endast är tillgänglig för behöriga. **Riktighet**, inklusive **spårbarhet**, innebär att informationen är korrekt och oförändrad samt att åtkomst och förändringar kan följas och verifieras när det behövs. **Tillgänglighet** säkerställer att informationen kan nås och användas när behov uppstår. Dessa principer används som grund för att identifiera risker, bedöma konsekvenser av bristande skydd och fastställa adekvata skyddsåtgärder.

Riskhantering som en sammanhängande process



Figur 1 – Samband mellan olika element i riskhanteringsprocessen.

Beskrivning

Relationen mellan elementen kan beskrivas som:

- Information tillhör informationsklass K: [t.ex. 3], R: [t.ex. 1], T: [t.ex. 2] som ställer krav på säkerhetsåtgärd.
- Säkerhetsåtgärd skyddar information.
- Information utsätts för risk.
- Sårbarhet och hot påverkar risk.
- Hot utnyttjar sårbarhet.
- Hotaktör använder attackmetod som realiserar hot.
- Säkerhetsåtgärd förändrar risk.

Informationsklassning

Inledande information

I detta avsnittet finns information om:

- Vad informationsklassning är.
- När en informationsklassning kan behöva genomföras.
- Information om klassningsmodellen som styr klassificeringen.
- Vad som behöver förberedas inför en informationsklassning.
- Hur en informationsklassning genomförs.
- Vad som ska genomföras efter en informationsklassning.

Vad är informationsklassning?

Informationsklassning är en metod som används för att bedöma hur skyddsvärd information är. Syftet är att avgöra vilken säkerhetsnivå som krävs utifrån hur allvarliga konsekvenser det skulle få om informationen blir obehörigt spridd (konfidentialitet), blir felaktig eller förändrad och inte går att spåra (riktighet inklusive spårbarhet) eller blir otillgänglig när den behövs (tillgänglighet).

När en informationsklassning ska genomföras

All information ska klassas för att ge en tydlig bild av vilken information som finns, hur den flödar inom verksamheten och vilket skydd den kräver. Som en första prioritet är rekommendationen att verksamheterna börjar med att klassa informationen i sina mest kritiska system och vid anskaffning eller upphandling av nya system och tjänster.

Övriga exempel på situationer då en informationsklassning ska genomföras är:

- Vid **identifiering** av system som inte har klassats.
- Vid **förändringar** som kan påverka säkerheten i system och tjänster. Exempelvis vid ändringar i systemets funktionalitet eller integrationer men även vid leverantörsbyte.
- När **IT-drift ska läggas ut** (outsourcas).
- Vid **förändringar i omvärlden** som påverkar hotbilden av information eller vid nyupptäckta sårbarheter.

Klassningsmodell

Klassningsmodellen är ett beslutat dokument som informationssäkerhetsarbetet grundar sig på och som används i klassningsarbetet. Modellen består av olika konsekvenskategorier, konsekvensnivåer och en klassningsmatris. Information ska klassas utifrån de konsekvenser i klassningsmodellen som otillräckligt skydd (utifrån konfidentialitet, riktighet och tillgänglighet) av informationen skulle kunna få för kommunen.

Varje område bedöms utifrån en femgradig skala (även kallat konsekvensnivåer):

0. *Försumbar.*
1. *Måttlig.*
2. *Betydande.*
3. *Allvarlig.*
4. *Betydelse för Sveriges säkerhet.*

Konsekvensnivåerna fastställer hur allvarliga följderna kan bli vid bristande skydd.

Konsekvenskategorierna som kommunen beslutat om är:

- Ekonomisk skada.
- Negativ påverkan på verksamheten.
- Bristande lagefterlevnad.
- Förtroendeskada.
- Påverkan på liv och hälsa.
- Påverkan på enskildas fri- och rättigheter (integritet).

Klassningsmodellen finns att hitta på kommunens intranät.

Hur ska klassningsmodellen tillämpas?

Klassningsmodellen tillämpas genom att deltagarna steg för steg bedömer vilka konsekvenser det kan få om informationens konfidentialitet, riktighet eller tillgänglighet inte skyddas. För varje konsekvens avgör deltagarna också hur allvarlig konsekvensen är genom nivåerna försumbar till betydelse för Sveriges säkerhet.

Exempel på tillämpning

- Ett fel i ett IT-system kan leda till att utbetalningar av ekonomiskt stöd försenas, vilket påverkar både verksamheten och enskilda personer på en allvarlig nivå (3).
- Om information inte är tillgänglig kan det uppstå behov av kostsamma reservrutiner – en ekonomisk konsekvens som kan vara på en betydande nivå (2).
- Inkorrekt förändringar i information kan leda till felaktiga beslut vilket kan ha allvarlig påverkan på liv och hälsa (nivå 3).

- Obehörigt röjande av information kan innebära att kommunen brister i lagefterlevnad och äventyrar Sveriges rikes säkerhet (nivå 4).
- Om informationen är otillgänglig innebär det en negativ påverkan för verksamheten i försumbar omfattning (nivå 0).

Det räcker att en av principerna bedöms som t.ex. allvarlig (3) vid bristande skydd för att informationen ska få den klassificeringen.

Förbered informationsklassning

1. Initiera

När behovet av att utföra en informationsklassning uppstår är det informationsansvariges ansvar att initiera informationsklassningen. Informationsansvarig ansvarar för att initiera klassningen genom att ta kontakt med den utvalda workshopledaren eller förvaltningens informationssäkerhets- och dataskyddskoordinator (se beskrivning under rubriken ”2. Bestäm deltagare”). Workshopledaren ansvarar vidare för att:

- Registrera ett ärende i Ciceron där alla handlingar ska infogas.
- Boka ett informationsklassningsmöte med övriga bestämda deltagare (enligt avsnitt ”2. Bestäm deltagare”).
- Infoga underlaget som hämtats (under avsnitt ”3. Hämta underlag”) i mötesbokningen och i Ciceron.

2. Bestäm deltagare

För att en informationsklassning ska bli effektiv och ge ett tillförlitligt resultat är det viktigt att rätt personer deltar i arbetet. Följande roller och funktioner kan vara relevanta:

- **Workshopledare:** Ansvarar för att leda och strukturera arbetet när verksamheten klassar sin information. Rollen innebär inte att fatta beslut, utan att stödja processen. Vilken funktion som är workshopledare beror på vilken information som ska klassas. Det kan vara en projektledare, informationssäkerhets- och dataskyddskoordinator, systemägare, systemförvaltare, upphandlare m.m. Workshopledaren tilldelas behörighet till verktyget Klassa 4.0.
- **Anteckningsstöd:** Stödjer processen genom att dokumentera diskussioner och beslut under workshopen.
- **Chefer eller verksamhetsrepresentanter:** Bidrar med insikt i vilken information som hanteras, hur den används och vilka konsekvenser brister i konfidentialitet, riktighet eller tillgänglighet kan få. Detta kan vara systemägare, systemförvaltare, medarbetare som arbetar i ett särskilt system eller arbetar med informationen som ska klassas, m.m.

2.1 Rekommenderade funktioner

Det är rekommenderat att inkludera medarbetare som har god kännedom om de regelverk som informationen omfattas av. Regelverken påverkar hur informationen ska värderas samt hanteras och medarbetare med sådan kunskap hjälper till att säkerställa att gällande lagar och regler följs.

Det är också rekommenderat att inkludera medarbetare med teknisk kompetens, till exempel från IT-enheten. De kan bidra med förståelse för hur informationen hanteras och skyddas tekniskt samt säkerställa att föreslagna åtgärder är genomförbara.

2.2 Stödfunktioner

Roller och funktioner som beskrivs nedan stöttar kommunens verksamheter i arbetet med riskhantering.

Informationssäkerhetssamordnare: Leder kommunens informationssäkerhetsarbete och stöttar under riskhanteringen genom att ge vägledning och säkerställa att arbetet följer metodstödet.

Informationssäkerhets- och dataskyddskoordinator: Arbetar operativt och stöttar förvaltningen i riskhanteringsarbetet. Koordinatoren kan hjälpa till att genomföra själva klassningen, tolka skyddsnivåer, dokumentera resultat och säkerställa att både informationssäkerhets- och dataskyddsaspekter hanteras korrekt.

Dataskyddsbud: Leder kommunens dataskyddsarbete och stöttar med kunskap om personuppgifter samt ser till att riskhanteringen beaktar krav enligt dataskyddsförordningen (GDPR).

3. Hämta underlag

Underlaget används i syfte att skapa samförstånd om innehållet i den information klassningen avser. Följande underlag ska hämtas:

- Information från informationshanteringsplanen/tidigare kallat dokumenthanteringsplanen.
- Rättsliga krav på informationen.

Övrigt underlag som kan vara lämpligt att ta med (förutsatt att det finns) är tidigare klassningar som utförts av den information som ska klassas, en kartlagd beskrivning av processflödet för den information som ska klassas eller en teknisk beskrivning av t.ex. ett system.

Genomför informationsklassning

1. Inleda workshop

Börja workshopen med att gå igenom en beskrivning av informationen som ska klassas och sammanhanget. Målet är att skapa en gemensam förståelse för vad informationstillgången innefattar samt hur den är avsedd att användas och hanteras. Därefter är det lämpligt att kort introducera området informationssäkerhet och förklara syftet med informationsklassningar innan själva klassningsarbetet påbörjas.

2. Definiera klassningsobjekt

I det här steget handlar det om att ta reda på vilken information som ingår i det som ska klassas (att ”definiera klassningsobjektet”). Att definiera klassningsobjektet genomförs med stöd av Motala kommuns ’mall för klassningsrapport> Del 1’. I mallen ska bland annat bakgrund, informationsägare, om informationen används inom en särskild process, integrationer om det berör ett system, övrig information för kännedom, m.m. anges. Alla som deltar bidrar med sin kunskap om informationen.

Syftet är att samla den information som ska klassas vid ett specifikt tillfälle inom ett tydligt definierat klassningsobjekt.

3. Verksamhets- och juridisk analys

I detta steg ska verksamhetens krav på informationstillgången fastställas och identifieras, inklusive de lagkrav som gäller för verksamheten och hanteringen av relevant information. Analyserna ger värdefull vägledning om vilken miniminivå som bör tillämpas för aspekterna konfidentialitet, riktighet och tillgänglighet.

I klassningsverktyget Klassa 4.0 finns vissa författningar som man kan fylla i om informationen omfattas av särskilda lagkrav. Detta ska anges tillsammans med motivering. Observera att informationen kan omfattas av regelverk som inte finns i Klassa 4.0. Dessa ska noteras i klassningsrapporten.

Samtliga krav inklusive de som dokumenteras i Klassa 4.0 ska anges i klassningsrapporten under ”interna krav” och ”juridisk analys”.

4. Kris- och kontinuitetsanalys

Utifrån ett kris- och kontinuitetsperspektiv är det rekommenderat att göra bedömningar av hur länge informationen kan vara otillgänglig. Det är även bra att bedöma hur gammal informationen får vara vid återläsning efter till exempel ett IT-haveri.

5. Klassa information

När ni har gått igenom underlaget, kartlagt informationen och genomfört samtliga analyser ska ni klassa informationen. Detta kan också ske löpande i samband med respektive steg. Informationsklassningen ska genomföras i verktyget Klassa 4.0 med stöd av Motala kommuns klassningsmodell. Motivering och nivå på konfidentialitet, riktighet samt tillgänglighet ska anges i Klassa 4.0 och i klassningsrapporten under ”informationsklassning och motivering”. Nivån på varje aspekt sätts med stöd av de konsekvenser i klassningsmodellen som kan drabba informationen vid brister i konfidentialitet, riktighet och tillgänglighet.

Frågor att ställa under klassningen utifrån informationssäkerhetsprinciperna är:

- **Konfidentialitet:** Vilka konsekvenser utifrån klassningsmodellen drabbar verksamheten ifall informationen skulle röjas till obehöriga? Hur allvarliga är konsekvenserna sett till nivåerna försumbar till betydelse för Sveriges säkerhet?
- **Riktighet inklusive spårbarhet:** Vilka konsekvenser utifrån klassningsmodellen drabbar verksamheten ifall informationen skulle ändras felaktigt? Vilka konsekvenser får det ifall ändringar inte kan spåras? Hur allvarliga är konsekvenserna?
- **Tillgänglighet:** Vilka konsekvenser utifrån klassningsmodellen drabbar verksamheten ifall informationen inte skulle finnas tillgänglig när den behövs? Hur allvarliga är konsekvenserna?

5.1 Upphandlingskrav

Efter genomförd informationsklassning genererar Klassa 4.0 en lista med förslag på informationssäkerhetskrav som kan användas i samband med en upphandling. Listan på informationssäkerhetskrav behöver gås igenom för att bedöma vilka krav som passar i sammanhanget.

5.2 Handlingsplan

Efter informationsklassningen kan du göra en självskattning som visar vilka åtgärder som behöver vidtas och vilka som redan är genomförda. Resultatet kan tas ut som en handlingsplan som kan användas både i det praktiska arbetet med förvaltning av enskilda verksamhetssystem och i det systematiska kvalitetsarbetet på övergripande nivå. Kraven som finns i handlingsplanen är huvudsakligen ställda mot kommunen och är åtgärder som kommunen behöver vidta för att skydda informationen. Vissa krav kan dock beröra leverantörer. Till exempel beroende på driftsform av ett system. Om systemet är lokalt, så riktas särskilda krav mot kommunens IT-enhet; om systemet är externt, så riktas kraven mot leverantören.

5.3 Tröskelanalys för konsekvensbedömning avseende dataskydd

En konsekvensbedömning avseende dataskydd är obligatorisk om en personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. För att bedöma om det krävs en konsekvensbedömning genomförs en tröskelbedömning med stöd av särskilda frågor. Fyll i frågorna i mallen för klassningsrapporten som berör tröskelbedömning för att avgöra om personuppgiftsbehandlingen kräver en konsekvensbedömning.

Arbete efter informationsklassning

1. Rapportera resultat

I detta steg ska resultatet rapporteras till informationsansvarige som beställt informationsklassningen. Innan rapporteringen sker behöver workshopledaren säkerställa att alla delar i Klassa 4.0 har besvarats, att dokumentationen i klassningsrapporten är fullständig samt kontrollera eventuella stavfel, formaliteter och liknande. Eventuella bilagor ska bifogas, och relevant underlag kopplat till klassningsresultatet ska inkluderas. Informationsansvarig ska därefter bekräfta och dokumentera att klassningsresultatet har fastställts och godkänts i klassningsrapporten.

Workshopledaren ska säkerställa att informationssäkerhets- och dataskyddskoordinatorn för den aktuella förvaltningen informeras om det finns ett behov av att registerförteckningen för behandling av personuppgifter uppdateras.

Informationsansvarige ansvarar därefter för att agera i enlighet med syftet bakom klassningen, exempelvis att upprätta en riskanalys (se avsnitt ”riskanalys”), att formulera säkerhetskrav inför en upphandling och/eller bedöma om det befintliga skyddet av informationen är tillräckligt. Om det befintliga skyddet är otillräckligt ska säkerhetsåtgärder implementeras (se avsnitt ”val av åtgärder”).

2. Diarieför handlingar

Alla handlingar som skapas ska diarieföras i kommunens ärendehanteringssystem Ciceron i det ärendet som skapats av workshopledaren. Registreringen ska ske utan dröjsmål och följa gällande rutiner för allmänna handlingar. Vid diarieföring ska ärendemening och klassificering utformas så att känsliga uppgifter inte röjs. Eventuella sekretessbedömningar görs i samband med registrering.

Analyser efter informationsklassning

Risikanalys och val av säkerhetsåtgärder

När en informationsklassning är färdigställd kan nästa steg vara att en riskanalys behöver upprättas. Syftet är att identifiera risker kopplade till det område som analyseras samt att identifiera åtgärder som ska vidtas för att minska eller helt eliminera riskerna. Den informationsklassning som tagits fram utgör ett viktigt underlag vid genomförandet av en riskanalys.

Information i system som resulterar i ett klassningsvärde på minst 2 ska följas av en riskanalys. I praktiken innebär det att en riskanalys behövs för system med information som t.ex. får klassningsvärdet K1: R2: T1, medan system med information som får klassningsvärdet K0: R1: T1 inte nödvändigtvis kräver en riskanalys.

Att en riskanalys inte krävs innebär dock inte att säkerhetsåtgärder kan uteslutas. Även information med låg klassning kan ha behov av grundläggande säkerhetsåtgärder, se avsnittet "Val av säkerhetsåtgärder" nedan. Riskanalysen är alltså det verktyg som används för att identifiera ytterligare eller mer specifika åtgärder när klassningen motiverar det, inte den enda vägen till att säkerhetsåtgärder överhuvudtaget vidtas.

Konsekvensbedömning avseende dataskydd (DPIA)

Om den genomförda tröskelbedömningen resulterar i en hög sannolikhet för att fysiska personers fri- och rättigheter riskeras ska en konsekvensbedömning göras.

Risikanalys

Inledande information

I detta avsnittet finns information om:

- Vad en riskanalys är.
- När en riskanalys ska genomföras.
- Vad som behöver förberedas inför en riskanalys.
- Hur en riskanalys ska genomföras.
- Arbete efter en riskanalys.

Övergripande information

Risikanalys är en central del i det systematiska informationssäkerhetsarbetet. Förutsättningarna för säker hantering av information förändras ständigt - nya risker tillkommer och identifierade risker förändras. Att arbeta med riskanalyser innebär att kommunen har ett enhetligt arbetssätt för att identifiera, analysera, värdera, behandla och följa upp risker så att kommunen över tid kan upprätthålla en tillräcklig nivå av informationssäkerhet. Riskanalyser används för att anpassa skyddet till verksamhetens informationstillgångar. Känner vi inte till vilka risker som finns är det svårt att utforma ett säkert och kostnadseffektivt skydd.

Syfte

Syftet med en riskanalys är att identifiera situationer som kan hindra organisationen från att nå sina mål och ge ett underlag för att välja lämpliga säkerhetsåtgärder samt öka medvetenheten om de risker som är kopplade till den analyserade informationen. Riskanalyser behöver även genomföras för att kommunen ska efterleva de krav som ställs.

Mål

En riskanalys går ut på att besvara tre grundläggande frågor: Vilka oönskade händelser kan inträffa? Vilka konsekvenser får de? Och hur sannolikt är det att de inträffar?

Målet med riskanalyser är att identifiera **hot**, **sårbarheter** och **risker**:

- Hot** är något som kan orsaka skada på informationen, systemet eller verksamheten.
- Sårbarhet** är en svaghet i skyddet av informationen, systemet eller verksamheten.

- iii. **Risk** är sannolikheten att ett hot utnyttjar en sårbarhet och orsakar skada eller förlust av informationen.

När ska en riskanalys genomföras?

Riskanalysen kan ses som en fortsättning på informationsklassningen eftersom det redan vid klassningen ofta kommer fram vad som skulle hända vid brister i konfidentialitet, riktighet och tillgänglighet. Till skillnad från en informationsklassning tar en riskanalys också hänsyn till sannolikheten för olika händelser.

System eller information som resulterar i ett klassningsvärde på minst 2 ska följas av en riskanalys. I praktiken innebär det att en riskanalys behövs för system med information som får klassningsvärdet K1: R2: T1 medan system med information som får klassningsvärdet K0: R1: T1 inte nödvändigtvis kräver en riskanalys.

Metod för genomförande

En riskanalys kan antingen genomföras med hjälp av en workshop där flera personer deltar men kan även (för mindre riskanalyser) genomföras i ”skrivbordsform” med enbart en eller ett par personer. Det är avgörande att rätt mängd resurser med rätt kompetens deltar. Tänk på att för stora grupper inte alltid arbetar effektivt och att det då kan vara nödvändigt att dela in gruppen i undergrupper.

Förbereda

1. Utse deltagare

En riskanalys ska genomföras av personer med relevant kunskap om verksamheten och den information som ska analyseras. Rollerna liknar dem som deltar vid informationsklassning, men för riskanalyser kan det vara bra att involvera medarbetare med särskild kompetens som t.ex. teknisk. Ansvar och förslag på roller finns i avsnittet ”Informationsklassning”>”Förbereda informationsklassning”>”2. Bestäm deltagare”.

2. Hämta underlag inför riskanalys

Följande underlag kan vara lämpliga att ha med vid riskanalyser:

- Rättsliga krav på informationen.
- Resultat av informationsklassning.
- Dokumentation över teknisk plattform (förutsatt att detta finns).

Dessutom utgör resultat från granskningar och relaterade analyser viktiga underlag, exempelvis från revisioner, tidigare genomförda riskanalyser och inte minst inträffade incidenter.

Genomföra

1. Identifiera

Risker kan identifieras genom brainstorming där deltagarna utifrån sin kunskap och roll diskuterar möjliga informationssäkerhetsrisker, hot och sårbarheter. Riskanalysen ska vara heltäckande i bemärkelsen att den ska fånga alla typer av hot som kan drabba just den informationen, oavsett om hotet i grunden är fysiskt, tekniskt, personalrelaterat eller organisatoriskt. Alla idéer dokumenteras tydligt så att gruppen kan se och diskutera dem. Syftet är att samla in så många perspektiv och risker som möjligt innan någon prioritering eller analys görs.

Identifierade risker ska formuleras på ett tydligt sätt. Det är rekommenderat att de formuleras enligt följande regel:

Risk för [hot/sårbarhet] mot [information] som leder till [konsekvens].

Ett exempel på en formulering enligt denna regeln är: "Risk för [felaktig behörighetstilldelning] till [journalinformation] som kan leda till [att obehörig tar del av information som kan medföra förlust av konfidentialitet för information som omfattas av sekretess och tystnadsplikt]."

För att komma igång kan följande frågor vara till hjälp: "vad kan bli ett problem?", "vad skulle vara obehagligt om det hände?", "vad skulle göra att du inte sov gott på natten?"

Varje identifierad risk ska dokumenteras i mallen för riskanalys och åtgärder.

2. Värdera

Under det andra momentet handlar det om att värdera alla identifierade risker. Värderingen av identifierade risker består av två delar: konsekvens och sannolikhet.

2.1 Konsekvens

Den första delen handlar om att bedöma konsekvenserna av att de identifierade riskerna inträffar. Som stöd för detta ska Motala kommuns klassningsmodell användas. Deltagarna ska, utifrån klassningsmodellen, bedöma vilka konsekvenser inklusive allvarlighetsgrad respektive risk kan innebära. Observera att mallen för riskanalys och åtgärder innehåller nivåerna *försumbar* till *allvarlig*. Upptäcker arbetsgruppen att en risk har betydelse för Sveriges rikes säkerhet ska detta inte dokumenteras i den angivna mallen utan hanteras enligt särskild ordning och eskaleras till säkerhetschef alternativt närmaste chef.

2.2 Sannolikhet

Den andra delen av värderingen innebär att bedöma sannolikheten för att de identifierade riskerna inträffar. Bedömningen genomförs med hjälp av sannolikhetsnivåerna nedan.

Nivå		Intervall/förväntad frekvens
4	Mycket hög	<1 månad
3	Hög	1 månad - 1 år
2	Medel	1 - 10 år
1	Låg	>10 år

Ett sätt att bedöma sannolikhetsnivån är att reflektera över om risken har inträffat tidigare och hur ofta. Det är lämpligt att överväga om sannolikheten för att risken ska inträffa har ökat med det aktuella världsläget.

3. Prioritera

När konsekvens- och sannolikhetsnivån fastställts, ska ett riskvärde sättas för varje risk. Genom att ta fram ett riskvärde blir det enklare att prioritera vilka risker som ska behandlas först. Riskvärdet sätts automatiskt i mallen för riskanalys och åtgärder. Riskvärdet baseras på matrisen nedan.

Allvarlig	M	H	H	EH
Betydande	M	M	H	H
Måttlig	L	M	M	H
Försumbar	L	L	M	M
Kons./Sann.	Låg	Medel	Hög	Mycket hög

Vem som kan besluta om att acceptera en risk och vad som krävs för beslutet framgår av kommunens riskacceptanskriterier, se Gemensamma anvisningar för riskhantering av information.

Exempelfall

Riskvärdet bestäms av allvarlighetsgraden på konsekvensen (från försumbar - allvarlig) och sannolikhetsnivån (från låg – extremt hög). Exempel på detta presenteras nedan.

Risk	• Risk att fel person får tillgång till ett system.
Konsekvens	• Risk kan påverka enskildas fri och rättigheter (integritet) på betydande nivå enligt klassningsmodell.
Sannolikhet	• Sannolikheten att en sådan risk inträffar kan bedömas vara hög enligt sannolikhetsnivåerna i metodstödet.
Riskvärde	• Riskvärdet fastställs till hög risknivå enligt riskmatrisen.

Arbete efter riskanalys

1. Åtgärdsplan

När riskanalysen är genomförd är nästa steg att upprätta en åtgärdsplan med stöd av avsnittet ”Val av säkerhetsåtgärder”. Åtgärdsplanen ska tydligt ange vilka risker som ska hanteras, vilka åtgärder som ska vidtas, vem som ansvarar för genomförandet och tidsplan för åtgärderna. Åtgärdsplanen fungerar som underlag för uppföljning och säkerställer att identifierade risker hanteras på ett strukturerat sätt. Åtgärdsplanen dokumenteras i mallen för riskanalys och åtgärder.

2. Diarieför handlingar

Alla handlingar som skapas ska diarieföras i kommunens ärendehanteringssystem, Ciceron, under det ärende som öppnades i förberedelsefasen av informationsklassningen. Registreringen ska ske utan dröjsmål och följa gällande rutiner för allmänna handlingar. Vid diarieföring ska ärendemening och klassificering utformas så att känsliga uppgifter inte röjs. Har dokumentationen högt skyddsvärde kan en osäker lagringsplats innebära att kommunens informationssäkerhet äventyras. Eventuella sekretessbedömningar görs i samband med registrering.

Val av säkerhetsåtgärder

Inledande information

Nästa del i arbetet med riskhantering är att bedöma om det finns några befintliga åtgärder på plats och om de bedöms vara tillräckliga. De risker och konsekvenser efter en informationsklassning och riskanalys resulterat i ska åtgärdas på något sätt.

Avsnittet innehåller information om:

- Vad en säkerhetsåtgärd är.
- Hantering av risker.
- Välja säkerhetsåtgärd.

Vad är en säkerhetsåtgärd?

En säkerhetsåtgärd är en åtgärd som implementeras för att minska risker. En säkerhetsåtgärd kan skydda mot brister i konfidentialitet, riktighet eller tillgänglighet, eller mot flera av dessa samtidigt. När åtgärder identifieras är det därför viktigt att tänka på vilka aspekter av informationssäkerheten de skyddar.

Säkerhetsåtgärder kan vara administrativa, mänskliga, tekniska eller fysiska. Olika säkerhetsåtgärder behöver oftast kombineras för att ge informationen tillräckligt skydd.

Administrativ säkerhetsåtgärd

En administrativ säkerhetsåtgärd kan t.ex. vara regler, rutiner och policys som styr hur information ska hanteras på ett säkert sätt. Detta kan exempelvis vara policys för informationssäkerhet, rutiner för behörighetstilldelning eller rutiner för incidentrapportering.

Mänsklig säkerhetsåtgärd

En mänsklig säkerhetsåtgärd fokuserar på människors beteende och kunskap. Det kan exempelvis handla om utbildnings- och informationsinsatser, återrapporering och övningar för att höja kunskapen kring informationssäkerhet.

Teknisk säkerhetsåtgärd

En teknisk säkerhetsåtgärd handlar om att skydda information med hjälp av teknik. Det kan till exempel vara brandväggar som hindrar obehörig åtkomst, kryptering som skyddar data eller antivirusprogram som upptäcker skadlig kod.

Fysisk säkerhetsåtgärd

En fysisk säkerhetsåtgärd syftar till att skydda den fysiska miljön där information finns. Det kan vara låsta serverrum, passerkortssystem, övervakningskameror eller brandskydd.

Hantering av identifierade risker

Risker kan hanteras genom att:

- Accepteras, vilket innebär att risken bibehålls.
- Undvikas, genom att exempelvis avbryta en befintlig eller planerad aktivitet.
- Överförs, exempelvis genom att teckna en försäkring som täcker kostnaden för delar eller hela konsekvensen av att risken inträffar.
- Reduceras, genom säkerhetsåtgärder.

Hur identifierade risker hanteras beslutas av informationsansvarig. Vem som kan besluta om att acceptera en risk och vad som krävs för beslutet framgår av kommunens riskacceptanskriterier, se Gemensamma anvisningar för riskhantering av information.

Välja säkerhetsåtgärder

Vid val av säkerhetsåtgärder är det viktigt att se över vilka åtgärder som verksamheten eller kommunen redan har och vilka som saknas. För de åtgärder som redan finns krävs en värdering av om de är tillräckliga. Säkerhetsåtgärder ska väljas med stöd av handlingsplanen och/eller upphandlingskraven som genereras i Klassa 4.0 (se avsnitt "Klassa information"). Säkerhetsåtgärder som föreslås i Klassa 4.0 behöver gås igenom för att bedöma vilka krav som passar i sammanhanget.

Åtgärder ska dokumenteras i mallen för riskanalys och åtgärder. En åtgärdsplan innehåller bland annat åtgärdsförslag, vem som är ansvarig för respektive åtgärd, när åtgärder ska vara genomförda och möjlighet att följa upp status för införandet av olika åtgärder. Informationsansvarig behöver fatta beslut om vilka risker som ska åtgärdas och vilka som inte behöver åtgärdas, därmed är det lämpligt att motivera varför en åtgärd ska genomföras.

Diarieför handlingar

Alla handlingar som skapas (bl.a. åtgärdsplan) ska diarieföras i kommunens ärendehanteringssystem, Ciceron, under det ärende som öppnades i förberedelsefasen av informationsklassningen.

Uppföljning

Informationshanteringen förändras konstant. Organisatoriska förändringar, teknisk utveckling eller förändrade hotbilder gör att klassningar och riskanalyser behöver ses över regelbundet. Risken är annars att dessa blir föråldrade och att skyddet inte står i proportion till verkligheten. Att genomföra regelbundna uppföljningar bidrar till att verksamheten har möjlighet att arbeta förebyggande och fånga upp förändringar.

Informationsklassningar och riskanalyser ska ses över minst en gång per år eller vid behov. Effekten av beslutade säkerhetsåtgärder ska utvärderas som en del av uppföljningen.