

**Informationssäkerhets-klassning och riskanalys**

**Instruktion**



Innehållsförteckning

[Dokumentinformation 3](#_Toc53559922)

[Versionshantering 3](#_Toc53559923)

[Bilagor till instruktion 3](#_Toc53559924)

[Instruktion för informationssäkerhetsklassning 4](#_Toc53559925)

[Målgrupp 4](#_Toc53559926)

[Identifiera informationstillgångar 5](#_Toc53559927)

[Klassning av informationstillgångar 5](#_Toc53559928)

[Klassningen bedöms utifrån fyra aspekter: 5](#_Toc53559929)

[Riskanalys 7](#_Toc53559930)

[Planera och genomför åtgärder 8](#_Toc53559931)

[Stöd för bedömning av skyddsnivå 9](#_Toc53559932)

[Stöd vid bedömning av information som omfattas av lagar 9](#_Toc53559933)

[Säkerhetsskyddslagstiftningen 9](#_Toc53559934)

[NIS-direktivet 9](#_Toc53559935)

[Dataskyddsförordningen (GDPR) 9](#_Toc53559936)

[Patientdatalagen och kompletterande föreskrifter 9](#_Toc53559937)

[Offentlighet och sekretesslagen (OSL) 9](#_Toc53559938)

[Tabell informationssäkerhetsklassning 10](#_Toc53559939)

# Dokumentinformation

|  |  |
| --- | --- |
| Titel | Instruktion informationssäkerhetsklassning och riskanalys |
| Dokumenttyp | Regler |
| Skapat av | Arbetsgruppen för strategiskt informationssäkerhetsarbete |
| Datum | 2020-10-14 |
| Senast ändrad | 2020-10-14 |
| Godkänt av | Marcus Matteby, IT-direktör |
| Version | 1.0 |

## Versionshantering

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Ändrad av | Kommentar |
| 1.0 | 2020-10-14 | Emelie Näs | Godkänt av Marcus Matteby, IT-direktör |
|  |  |  |  |

## Bilagor till instruktion

|  |  |
| --- | --- |
| Bilaga | Beskrivning |
| Matris för informationssäkerhetsklassning. | Matris som fastställer skyddsnivåer för Sundsvalls kommunkoncern.  |
| Mall för informationssäkerhetsklassning. | En mall för dokumentation av informationssäkerhetsklassning. Via mallen skapas det primära dokumentet som beskriver och håller ihop en informationstillgångs informationssäkerhetsklassning. |
| Mall för riskanalys. | En mall för dokumentation av riskanalys. |
| Lista över exempel på risker. | Ett dokument som innehåller exempel på risker som kan finnas. Listan kan användas som stöd vid informationssäkerhetsklassning och riskanalys. |

# Instruktion för informationssäkerhetsklassning

I *Strategi för trygghet och säkerhet i Sundsvalls kommun* nämns att ”vid hantering av information ska vi säkerställa ett ändamålsenligt skydd”. Genom att informationssäkerhetsklassa och genomföra riskanalyser av vår information uppnår vi detta. Det är också en viktig del i arbetet med att ha en långsiktig informationsförvaltning och ett systematiskt informationssäkerhetsarbete.

Syftet med denna instruktion är att hjälpa dig att bedöma vilken skyddsnivå informationen behöver och bedöma vilka risker som finns. Klassningen och riskanalysen kan sedan användas för att ställa rätt krav på hanteringen av informationen och vilka säkerhetsåtgärder som krävs för att skydda den, till exempel mot ett IT-system, leverantörer av ett IT-system eller tjänster. Resultatet är också en bra grund för kontinuitetsplanering och krisberedskap.



*Denna bild visar vilka delar i processen som* i*nstruktionen gäller.*

En bedömning av skyddsnivå och risker är föränderlig, därför behöver man revidera dessa regelbundet. Om man till exempel klassat och gjort en riskanalys av ett system, kan man se över skyddsnivån och risker i samband med att man reviderar systemförvaltningsplanen. När man gör den regelbundna översynen av informationshanteringsplanen är också ett exempel på när det är lämpligt att gå igenom skyddsnivå eller riskanalys.

## Målgrupp

Denna instruktion ska stötta dig som ska leda eller delta i en informationssäkerhetsklassning eller en riskanalys av en informationstillgång.

För att få bästa resultat vid en informationssäkerhetsklassning eller riskanalys rekommenderas att man genomför den i workshopform, där deltagare med olika kompetenser och perspektiv deltar.

Förslag på deltagare:

* **Workshopledare.** Person som leder workshopen. Bör ha kompetens inom informationssäkerhetsklassning.
* **Informationsägare.** Ägaren av informationstillgången eller objektet. Normalt också den som är beställare av informationssäkerhetsklassningen.
* **Tekniskt kunnig om systemet.** Teknisk kunskap och kompetens om systemet och driften av det.
* **Verksamhetskompetens.** Kompetenser som kan de verksamhetsprocesser som är berörda av informationstillgången eller systemet.
* **Dokumentationsansvarig.** Ansvarar för att dokumentera workshopen i mallarna för riktlinjerna.

## Identifiera informationstillgångar

Använd: Mall för informationssäkerhetsklassning.

Börja med att dokumentera vad informationssäkerhetsklassningen gäller. Det kan till exempel vara ett projekt, hel eller del av organisation, en process, ett IT-system, en databas eller en enskild informationstillgång. Tänk på att avgränsa informationsmängden som ska klassas så att den blir hanterbart.

Finns det tidigare informationssäkerhetsklassningar eller annan dokumentation kring informationen kan ni använda den. Dokumentera också vem som är informationsägare och eventuella avgränsningar.

## Klassning av informationstillgångar

Informationssäkerhetsklassning innebär att man värderar hur viktig informationen är för verksamheten och att informationstillgången tilldelas en skyddsnivå.

Genom informationssäkerhetsklassningen blir känslig och kritisk information identifierad. Därefter kan ni vidta åtgärder så att den känsliga och kritiska informationen får tillräckligt skydd, medans annan typ av information inte får onödigt mycket skydd med höga kostnader som följd.

Dokumentera resultatet i: Mall för informationssäkerhetsklassning.

### Klassningen bedöms utifrån fyra aspekter:

* **Konfidentialitet** – att innehåll i information (eller ibland dess existens) inte får göras tillgänglig eller avslöjas för obehöriga.
* **Riktighet** – att information inte förändras vare sig av obehöriga, av misstag eller på grund av funktionsstörning. Informationen ska vara tillförlitlig, korrekt och fullständig.
* **Tillgänglighet** – att informationstillgångar ska kunna utnyttjas i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.
* **Spårbarhet** – det ska vara möjligt att i efterhand härleda hur uppgifter har behandlats och vilka specifika aktiviteter som ägt rum i samband med detta, vilka förändringar som skett och vem som har haft åtkomst till informationstillgångarna.

Utifrån respektive aspekt behöver ni resonera kring vilka konsekvenser det skulle få för verksamheten om något inträffar.

#### Exempel på konsekvenskategorier:

* Ekonomisk förlust (exempelvis minskade intäkter, ökade kostnader, skada på tillgångar).
* Negativ påverkan på eller avbrott i den operativa verksamheten.
* Överträdelse eller inte efterleva rättsliga krav.
* Skadat varumärke eller minskat förtroende.
* Skada på annan organisation eller omgivande samhället.
* Personskada.
* Miljöskada.

|  |  |  |
| --- | --- | --- |
| **Händelse** | **Konsekvens** | **Skyddsnivå** |
| Vad händer om informationen på hemsidan inte är **riktig**? | Vi kan ge felaktiga anvisningar vilket kan innebära svårigheter och i vissa fall innebära kostnader för medborgare. Kan leda till ökad **arbetsbelastning**, **ersättningsanspråk** och **minskat** **förtroende** för kommunen. | ? |

*Tabellen visar exempel på beskrivning av konsekvenser orsakade av en händelse*.

Det finns lagstiftningar som omfattar alla våra verksamheter, men också verksamhetsspecifika lagar som ni kan behöva ta hänsyn till i bedömningen.

Stöd till klassningen i form av exempel på konsekvenser finns i slutet av dokumentet.

#### Sundsvalls kommunkoncern använder sig av skyddsnivåerna 0-4

1. **Ingen skyddsnivå.** Medför **ingen negativ påverkan** på egen eller annan organisation eller dess tillgångar, eller på enskild individ.
2. **Grundläggande skyddsnivå.** Medför **måttlig negativ påverkan** på egen eller annan organisation eller dess tillgångar, eller på enskild individ.
3. **Utökad skyddsnivå.** Medför **betydande negativ påverkan** på egen eller annan organisation eller dess tillgångar, eller på enskild individ.
4. **Hög skyddsnivå.** Medför **allvarlig negativ påverkan** på egen eller annan organisation eller dess tillgångar, eller på enskild individ.
5. **Mycket hög skyddsnivå** (enligt säkerhetsskyddslagstiftning). Kan medföra **skada** på Sveriges säkerhet.

Får informationen skyddsnivå 2 eller 3 finns ett skyddsvärde kring informationen. Vi rekommenderar då att ni genomför en riskanalys.

Uppfattar ni att informationen hamnar på skyddsnivå 4 behöver ni bedöma informationen utifrån säkerhetsskyddslagstiftningen. Ta då kontakt med en kunnig person inom säkerhetsskydd för att få hjälp.

Tänk på att om man har stora mängder med information som slås ihop (aggregeras) kan detta innebära att informationen behöver en högre skyddsnivå. Exempelvis kan en stor informationsmängd med skyddsnivå 3 höjas till nivå 4 och omfattas av säkerhetsskyddslagen.

## Riskanalys

Använd: Mall för riskanalys för att dokumentera riskerna.

Riskanalyser används för att anpassa skyddet till verksamhetens informationstillgångar. Känner ni inte till vilka risker som finns är det svårt att utforma ett säkert och kostnadseffektivt skydd. En riskanalys går ut på att besvara frågorna:

* Vad kan hända?
* Vilka blir konsekvenserna?
* Hur sannolikt är det?

Syftet med riskanalysen är att hitta hot, sårbarheter och risker.

* Hot är något som kan orsaka skada på informationstillgången, systemet eller verksamheten.
* Sårbarhet är en svaghet i skyddet av informationstillgången, systemet eller verksamheten.
* Risk är sannolikheten att ett hot utnyttjar en sårbarhet och orsakar skada eller förlust av informationstillgången.

|  |  |  |
| --- | --- | --- |
| **Hot**Vad kan hända? | **Sårbarhet/Brist**Vad kan orsaka att nåt inträffar? | **Risk** |
| Felaktig eller avsaknad av information kring system eller processer | Alla relevanta roller har inte deltagit i workshop kring informationssäkerhetsklassning och riskanalys | Om alla relevanta roller inte deltar i informationssäkerhetsklassning och riskanalys finns en risk för att hot och sårbarheter inte identifieras eller att det inte finns tillräckliga säkerhetsåtgärder på plats. |

*Tabellen visar ett exempel på beskrivning av hot, sårbarhet och risk.*

Riskanalysen kan ses som en fortsättning på informationssäkerhetsklassningen eftersom det redan vid klassningen ofta kommer fram vad som skulle hända om ni misslyckas med att hålla informationen konfidentiell, riktig, tillgänglig och spårbar.

Det går också att göra en riskanalys separat för att se om skyddet är tillräckligt för exempelvis:

* verksamheten som helhet.
* en särskild informationstillgång.
* en specifik applikation.
* en serverhall.
* en verksamhetsprocess.
* en organisationsförändring.
* en händelse, exempelvis vid införandet av ett nytt system.

Resultatet av riskanalysen är en dokumentation över hot som kan påverka informationen negativt. Dokumentationen kan ni sedan använda för att bedöma vilka skyddshöjande åtgärder ni behöver göra.

För att få hjälp att komma igång finns en lista med risker som ni kan utgå ifrån. Dokumentera sedan varje identifierad risk i mallen för riskanalys.

Bedöm hur sannolikt det är att risken inträffar och hur stora konsekvenserna skulle bli. Här kan ni utgå från konsekvenskategorierna som beskrivs i avsnittet Klassning av informationstillgångar. Exempel på konsekvenser finns i slutet av dokumentet.

För att få ett riktvärde för hur allvarlig en risk är kan ni göra en beräkning av riskvärdet (sannolikhet\*konsekvens), se mallen för riskanalys.

Ta också fram förslag på åtgärder och skriv ner dem i mallen. Åtgärder som rör ett IT-system bör ni överlämna till systemförvaltaren som dokumenterar detta i systemförvaltningsplanen.

## Planera och genomför åtgärder

Gör en bedömning av vilka risker ni ska åtgärda utifrån de risker och åtgärdsförslag som kommit fram i riskanalysen. Ni bör upprätta en handlingsplan för att få en bild över vilka åtgärder som är nödvändiga och vem som ansvarar för att genomföra dessa. Det är slutligen informationsägaren som beslutar om åtgärderna.

Ni kan använda verktyget KLASSA från SKL för att skapa en handlingsplan med åtgärder för informationstillgången. Verksamheten får då svara på ett antal frågor som genererar en generell och detaljerad handlingsplan.

***Tips!*** *KLASSA är ett mycket detaljerat verktyg med tyngdpunkt på teknisk säkerhet. Det är främst lämpligt för att identifiera krav på IT-stöd som finns i okänd miljö, till exempel en molntjänst. Om IT-stödet omfattas av det generella säkerhetsskyddet inom koncernens interna drifttjänster medföljer samtidigt en stor del skydd som KLASSA ställer krav på via de rutiner och skydd som ingår i de interna drifttjänsterna.*

# Stöd för bedömning av skyddsnivå

Följande information kan användas som stöd vid informationssäkerhetsklassning.

## Stöd vid bedömning av information som omfattas av lagar

Mer information om dessa lagar finns på https://klassa-info.skl.se/stodmaterial/page/vagledning.

### Säkerhetsskyddslagstiftningen

Hanteringen av säkerhetsskyddsklassificerade handlingar och uppgifter klassificeras som **synnerligen allvarlig** (nivå 4) för samtliga säkerhetsaspekter.

### NIS-direktivet

Mycket troligt hamnar tjänster eller system som omfattas av lagen i klassificeringen **allvarlig** (nivå 3) för samtliga säkerhetsaspekter.

Finns det skäl att tro att klassificeringen är **synnerligen allvarlig** (4) är det inte självklart att det är NIS-direktivet som är normerande utan snarare kan verksamheten då omfattas av Säkerhetsskyddslagstiftningen.

### Dataskyddsförordningen (GDPR)

Troligt hamnar personuppgifter i klassificeringen **betydande** (nivå 2) för samtliga säkerhetsaspekter.

I sammanhang där särskilda kategorier (känsliga personuppgifter) behandlas är klassificeringen **allvarlig** (nivå 3) för säkerhetsaspekten konfidentialitet och i vissa fall även riktighet.

### Patientdatalagen och kompletterande föreskrifter

Mycket troligt hamnar patientdata i klassificeringen **betydande** (nivå 2) för samtliga säkerhetsaspekter.

I sammanhang där särskilda kategorier (känsliga personuppgifter) behandlas är klassificeringen **allvarlig** (nivå 3)för säkerhetsaspekten konfidentialitet.

I sammanhang med mycket höga krav på riktighet, exempelvis ordinationer, är klassificeringen **allvarlig** (nivå 3) för säkerhetsaspekten riktighet.

### Offentlighet och sekretesslagen (OSL)

Mycket troligt hamnar information som är sekretessklassad enligt OSL i klassificeringen **betydande** (nivå 2). **allvarlig** (nivå 3) eller **synnerligen allvarlig** (nivå 4) när det gäller konfidentialitet.

## Tabell informationssäkerhetsklassning

|  |  |
| --- | --- |
| Nivå | Konfidentialitet |
| 0 | Röjande av informationen medför **ingen eller försumbar skada** för verksamheten eller enskilds personliga förhållanden.Informationen är avsedd för bred spridning och publicitet och innehåller inga personuppgifter. |
| 1 | Röjande av informationen medför **måttlig skada** för verksamheten eller enskilds personliga förhållanden.Informationen omfattar endast allmänna offentliga handlingar och är inte skyddsvärd och innehåller enstaka personuppgifter av ej känslig karaktär.Exempel på möjliga konsekvenser som kan uppstå:* Måttlig ekonomisk förlust för verksamheten. Avvikelse på cirka 5-10 procent av budget.
* Måttlig förtroendeförlust, enstaka missnöjda intressenter eller mindre notis i lokalmedia.
* Måttligt produktionsbortfall, mindre omprioriteringar i verksamheten, måttliga återställningskostnader i tid och pengar.
* Ingen personskada, lindriga hot och kränkningar.
 |
| 2 | Röjande av informationen medför **kännbar skada** för verksamheten eller enskilds personliga förhållanden.Informationen innehåller arbetshandlingar eller allmänna handlingar *som kan bli* föremål för sekretess enligt OSL. Information avsedd för internt bruk eller innehåller personuppgifter enligt GDPR.Exempel på möjliga konsekvenser som kan uppstå:* Betydande ekonomisk förlust, avvikelse på cirka 10-20 procent av budget.
* Betydande förtroendeförlust, uppmärksammas i riks- och lokalmedia, grupperingar på sociala medier. Dock begränsat till enskilda händelser eller enskilda personers agerande.
* Stort produktionsbortfall, stora omprioriteringar i verksamheten, höga återställningskostnader i tid och pengar.
* Lindrig personskada (fysisk eller psykisk) hos medborgare eller medarbetare, allvarliga hot och kränkningar.
 |
| 3 | Röjande av informationen medför **allvarlig skada** för verksamheten eller enskilds personliga förhållanden.Informationen innehåller uppgifter som är föremål för sekretess enligt OSL, känsliga personuppgifter, andra områdesspecifika lagstiftningar eller tystnadsplikt.Exempel på möjliga konsekvenser som kan uppstå:* Allvarlig ekonomisk förlust avvikelse på över 20 procent av budget.
* Allvarlig förtroendeförlust, ihållande drev i rikstäckande medier, eller av ej organiserade grupperingar på sociala medier. Hela organisationen och dess kultur pekas ut.
* Mycket stort produktionsbortfall, omfattande omprioriteringar i verksamheten, mycket höga återställningskostnader i tid och pengar.
* Svår personskada (fysisk eller psykisk)/dödsfall hos medborgare eller medarbetare.
 |
| 4 | Informationen omfattas av säkerhetsskyddslagen och röjande av information kan medföra skada för Sveriges säkerhet.Information med skyddsnivå 3 som slås ihop (aggregeras) kan omfattas av säkerhetsskyddslagenKontakta någon som är insatt i säkerhetsskydd och gör en bedömning utifrån den. |

|  |  |
| --- | --- |
| Nivå | Riktighet |
| 0 | Information som obehörigen, av misstag eller på grund av funktionsstörning ändrats medför **ingen eller försumbar skada** för verksamheten eller enskilds personliga förhållanden. |
| 1 | Information som obehörigen, av misstag eller på grund av funktionsstörning ändrats medför **måttlig skada** för verksamheten eller enskilds personliga förhållanden.Informationen innehåller uppgifter som med begränsad insats kan återställas. Förändringarna bedöms inte leda till negativ påverkan för verksamheten.Exempel på möjliga konsekvenser som kan uppstå:* Måttlig ekonomisk förlust för verksamheten. Avvikelse på cirka 5-10 procent av budget.
* Måttlig förtroendeförlust, enstaka missnöjda intressenter eller mindre notis i lokalmedia.
* Måttligt produktionsbortfall, mindre omprioriteringar i verksamheten, måttliga återställningskostnader i tid och pengar.
* Ingen personskada, lindriga hot och kränkningar.
 |
| 2 | Information som obehörigen, av misstag eller på grund av funktionsstörning ändrats medför **kännbar skada** för verksamheten eller enskilds personliga förhållanden.Informationen ingår i myndighetsutövningen eller innehåller uppgifter som omfattas av lagrum där riktighetskrav anges. Exempel på möjliga konsekvenser som kan uppstå:* Betydande ekonomisk förlust, avvikelse på cirka 10-2 procent av budget.
* Betydande förtroendeförlust, uppmärksammas i riks- och lokalmedia, grupperingar på sociala medier. Dock begränsat till enskilda händelser eller enskilda personers agerande.
* Stort produktionsbortfall, stora omprioriteringar i verksamheten, höga återställningskostnader i tid och pengar.
* Lindrig personskada (fysisk eller psykisk) hos medborgare eller medarbetare, allvarliga hot och kränkningar.
 |
| 3 | Information som obehörigen, av misstag eller på grund av funktionsstörning ändrats medför **allvarlig skada** för verksamheten eller enskilds personliga förhållanden.Informationen innehåller uppgifter där hanteringen styrs av specifika lagparagrafer, känsliga personuppgifter eller hälso- och sjukvård. Exempel på möjliga konsekvenser som kan uppstå:* Allvarlig ekonomisk förlust avvikelse på över 20 procent av budget.
* Allvarlig förtroendeförlust, ihållande drev i rikstäckande medier, eller av ej organiserade grupperingar på sociala medier. Hela organisationen och dess kultur pekas ut.
* Mycket stort produktionsbortfall, omfattande omprioriteringar i verksamheten, mycket höga återställningskostnader i tid och pengar.
* Svår personskada (fysisk eller psykisk)/dödsfall hos medborgare eller medarbetare.
 |
| 4 | Information som obehörigen, av misstag eller på grund av funktionsstörning ändrats kan medföra skada på Sveriges säkerhet.Kontakta någon som är insatt i säkerhetsskydd och gör en bedömning utifrån den. |

|  |  |
| --- | --- |
| Nivå | Tillgänglighet |
| 0 | Ett avbrott medför **ingen eller försumbar skada** för verksamheten eller enskilds personliga förhållanden. |
| 1 | Ett avbrott medför **ingen, försumbar eller måttlig skada** för verksamheten eller enskilds personliga förhållanden.Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas endast i begränsad omfattning av otillgänglighet till informationen. Informationen kan vara otillgängligt i ett par dygn med måttlig inverkan på verksamheten.Exempel på möjliga konsekvenser som kan uppstå:* Måttlig ekonomisk förlust för verksamheten. Avvikelse på cirka 5-10 procent av budget.
* Måttlig förtroendeförlust, enstaka missnöjda intressenter eller mindre notis i lokalmedia.
* Måttligt produktionsbortfall, mindre omprioriteringar i verksamheten, måttliga återställningskostnader i tid och pengar.
* Ingen personskada, lindriga hot och kränkningar.
 |
| 2 | Ett avbrott medför **kännbar skada** för verksamheten eller enskilds personliga förhållanden.Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i betydande omfattning av otillgänglighet till information. Informationen kan vara otillgängligt i ett par timmar utan negativ inverkan på verksamheten.Exempel på möjliga konsekvenser som kan uppstå:* Betydande ekonomisk förlust, avvikelse på cirka 10-20 procent av budget.
* Betydande förtroendeförlust, uppmärksammas i riks- och lokalmedia, grupperingar på sociala medier. Dock begränsat till enskilda händelser eller enskilda personers agerande.
* Stort produktionsbortfall, stora omprioriteringar i verksamheten, höga återställningskostnader i tid och pengar.
* Lindrig personskada (fysisk eller psykisk) hos medborgare eller medarbetare, allvarliga hot och kränkningar.
 |
| 3 | Ett avbrott medför **allvarlig skada** för verksamheten eller enskilds personliga förhållanden.Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i allvarlig omfattning av otillgänglighet i systemet. Informationen kan vara otillgängligt i upp till en timme per åt utan negativ inverkan på verksamheten.Exempel på möjliga konsekvenser som kan uppstå:* Allvarlig ekonomisk förlust avvikelse på över 20 procent av budget.
* Allvarlig förtroendeförlust, ihållande drev i rikstäckande medier, eller av ej organiserade grupperingar på sociala medier. Hela organisationen och dess kultur pekas ut.
* Mycket stort produktionsbortfall, omfattande omprioriteringar i verksamheten, mycket höga återställningskostnader i tid och pengar.
* Svår personskada (fysisk eller psykisk)/dödsfall hos medborgare eller medarbetare.
 |
| 4 | Ett avbrott kan medföra skadapå Sveriges säkerhet.Kontakta någon som är insatt i säkerhetsskydd och gör en bedömning utifrån den. |

|  |  |
| --- | --- |
| Nivå | Spårbarhet |
| 0 | Att spårbarhet saknas medför **ingen skada** för verksamheten eller enskilds personliga förhållanden.Exempel information. |
| 1 | Att spårbarhet saknas medför **ingen, försumbar eller måttlig skada** för verksamheten eller enskilds personliga förhållanden.Möjligheten att härleda vad som har hänt med informationen vid förändringar av uppgifter, incident eller säkerhetsincident bedöms vara oviktigtExempel på möjliga konsekvenser som kan uppstå:* Måttlig ekonomisk förlust för verksamheten. Avvikelse på cirka 5-10 procent av budget.
* Måttlig förtroendeförlust, enstaka missnöjda intressenter eller mindre notis i lokalmedia.
* Måttligt produktionsbortfall, mindre omprioriteringar i verksamheten, måttliga återställningskostnader i tid och pengar.
* Ingen personskada, lindriga hot och kränkningar.
 |
| 2 | Att spårbarhet saknas medför **kännbar skada** för verksamheten eller enskilds personliga förhållanden.Möjligheten att härleda vad som har hänt med informationen vid förändringar, incident eller säkerhetsincident bedöms vara viktigt. Spårbarhet ska finnas för att påvisa på vilket sätt information har behandlats och av vem.Exempel på möjliga konsekvenser som kan uppstå:* Betydande ekonomisk förlust, avvikelse på cirka 10-20 procent av budget.
* Betydande förtroendeförlust, uppmärksammas i riks- och lokalmedia, grupperingar på sociala medier. Dock begränsat till enskilda händelser eller enskilda personers agerande.
* Stort produktionsbortfall, stora omprioriteringar i verksamheten, höga återställningskostnader i tid och pengar.
* Lindrig personskada (fysisk eller psykisk) hos medborgare eller medarbetare, allvarliga hot och kränkningar.
 |
| 3 | Att spårbarhet saknas medför **allvarlig skada** för verksamheten eller enskilds personliga förhållanden.Möjligheten att härleda vad som har hänt med informationen vid förändringar, incident eller säkerhetsincident bedöms vara mycket viktigt. Spårbarhet ska finnas för alla specificerade händelser.Exempel på möjliga konsekvenser som kan uppstå:* Allvarlig ekonomisk förlust avvikelse på över 20 procent av budget.
* Allvarlig förtroendeförlust, ihållande drev i rikstäckande medier, eller av ej organiserade grupperingar på sociala medier. Hela organisationen och dess kultur pekas ut.
* Mycket stort produktionsbortfall, omfattande omprioriteringar i verksamheten, mycket höga återställningskostnader i tid och pengar.
* Svår personskada (fysisk eller psykisk)/dödsfall hos medborgare eller medarbetare.
 |
| 4 | Att spårbarhet saknas kan medföra skada för **skada** för Sveriges säkerhet.Kontakta någon som är insatt i säkerhetsskydd och gör en bedömning utifrån den. |