Gäller för: Västra Götalandsregionen
Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2024-08-05
Giltig till: 2028-07-24

Riskhantering för informationssäkerhet

Regional rutin 2024 – 2028

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehåll

Sammanfattning

Mål: Informationssäkerhetsrisker som kan påverka Västra Götalandsregionens informationstillgångar och de registrerades integritet ska identifieras, analyseras, behandlas och följas upp.

Informationssäkerhet ska utgå från ett riskbaserat arbetssätt, vilket innebär att identifiera, analysera och bedöma risker mot verksamhetens informationstillgångar.

En informationssäkerhetsrisk är möjligheten för ett hot att utnyttja en sårbarhet hos en informationstillgång och därigenom orsaka verksamheter eller individer skada.

Det riskbaserade arbetssättet ska vara en integrerad del av ordinarie verksamhetsplanering med syfte att:

- ge en ökad medvetenhet om risker i verksamheten och för den personliga integriteten, och vilka säkerhetsåtgärder som krävs för att hantera dom,
- öka sannolikheten för organisationen att nå informationssäkerhetsmålen samt
- hantera risker till en acceptabel nivå.

Rutinen är styrande för alla förvaltningar och bolag i Västra Götalandsregionen (VGR) och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD). Rutinen fastställer den process och bedömningsmetod som ska användas för riskhantering mot informationssäkerhetsmålen, vilket inkluderar perspektiven informationssäkerhet och personlig integritet avseende dataskydd.

1 Ansvar

Ansvaret för riskhanteringen följer linjen, vilket innebär att respektive förvaltningschef ska integrera riskhantering och dess aktiviteter i ordinarie verksamhet. Riskhantering ska vara en integrerad del av verksamheten och är en del av ledningens ansvar. Arbetet ska dokumenteras, följas upp och det ska vara tydligt vilka beslut som fattats och av vem.

1.2 Riskägare

För varje identifierad risk ska en riskägare identifieras som har befogenhet att hantera risken och fatta beslut om säkerhetsåtgärder.

Riskägare är ägare av de risker som informationstillgångarna utsätts för.

Riskägaren behöver inte vara den som utför och implementerar säkerhetsåtgärder för att hantera risk, men ska vara den som kan besluta, prioritera och resurssätta.

Riskägaren har att bedöma om informationssäkerhetsrisker har en regional påverkan och/eller påverkar verksamheter utöver eget mandat. Om så är fallet kan riskägaren få stöd i vart risken ska eskaleras genom att kontakta informationsstyrningsrådet på koncernkontoret.

1.3 Åtgärdsansvarig

Alla åtgärder ska kopplas till en åtgärdsansvarig, det är den person i organisation som har ansvar för att hantera åtgärden för risken inom fastställd tidplan. Denna kan vara riskägaren. I uppdraget ligger även ansvar för att återrapportera till riskägaren när åtgärd är utförd alternativt inte kunnat utföras enligt plan.

1.4 Särskilt utpekade ansvar

Riskhantering i projekt/uppdrag

Projektägaren eller uppdragsansvarig är ytterst ansvarig för att projektet/uppdraget bedriver ett strukturerat informationssäkerhetsarbete. Projektet/uppdraget ska analysera vilka informationssäkerhetsrisker som uppstår med anledning av initiativet. Vid avslut ska resultatet av riskhanteringen överlämnas till linjen. Det ska därmed finnas en utsedd riskägare i linjen som är mottagare av resultatet.

Koncernstab digitalisering

För IS/IT-tjänster ansvarar ägare av IS/IT-tjänsten att riskhantering genomförs.

Koncernstab digitalisering har ansvar för att övervaka och agera på informationssäkerhetsrisker i regionens IT-miljö (cybersäkerhetsrisker).

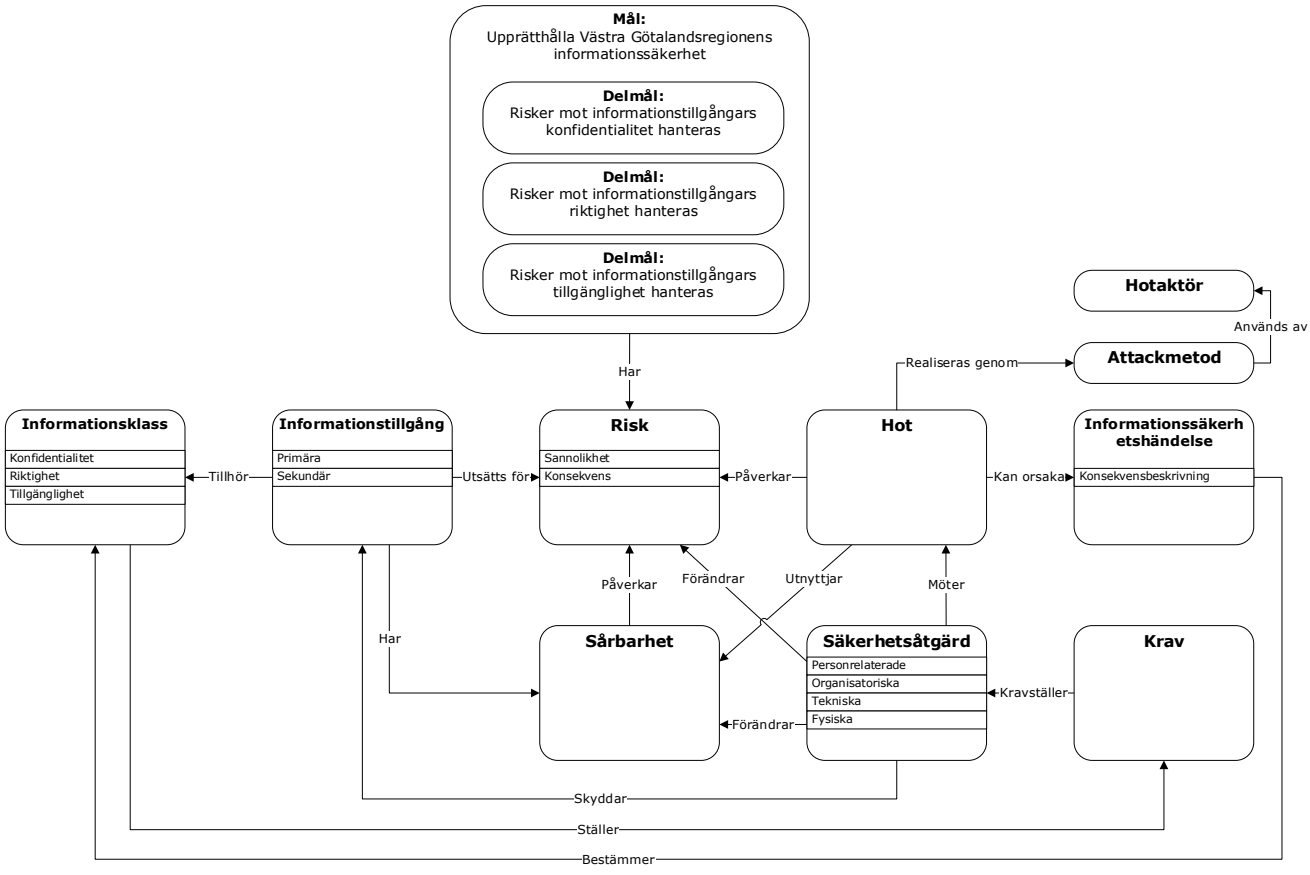
2 När riskhantering ska genomföras

Riskhantering ska alltid genomföras inför en ny situation eller en förändring, men också regelbundet, minst en gång per år även om det verkar som att ingen förändring har skett. Riskhantering ska vara en del av beslutsunderlag inför förändringar som påverkar informationshanteringen.

Exempel på tillfällen när processen för riskhantering alltid ska genomföras:

- vid anskaffning, upphandling eller avveckling av IS/IT-tjänster/drift,
- i samband med systemuppgraderingar, tekniska förändringar i infrastruktur eller programvaror,
- förändringar i omvärlden (tex förändrad hotbild, nyupptäckta sårbarheter),
- organisations-/processförändringar som kan påverka informationsbehandlingen eller
- när särskild lagstiftning ställer krav på att riskanalys och riskbedömning ska ligga till grund för beslut av hantering och åtgärder (till exempel PDL, NIS, GDPR)

3 Beskrivning av relationer för riskhantering



Figur 1 - Samband mellan olika element i riskhanteringsprocessen.

Relationen mellan elementen kan beskrivas som följer:

- En hotaktör använder en attackmetod för att realisera ett hot genom att utnyttja en sårbarhet.

- För att analysera risken med en potentiell informationssäkerhetshändelse behöver sannolikheten att hotaktören lyckas realisera hotet samt sannolikheten att incidenten orsakar den beskrivna konsekvensen bedömas.
- Informationssäkerhetsrisken kan sedan minskas genom att införa säkerhetsåtgärder som minskar sårbarheten eller mildrar konsekvenserna av en informationssäkerhetshändelse.

4 Bedömningsmetod

Vid bedömning ingår att

- uppskatta sannolikheten för att ett hot inträffar genom att använda skala för sannolikhet,
- uppskatta konsekvens utifrån skada på individ, verksamhet, samhällsviktig funktion och organisationens förtroende/ekonomi samt
- fastställa nivå för riskacceptans.

4.1 Skala för sannolikhet

När sannolikheten bedöms, hur troligt det är för risken att inträffa används nedanstående skala.

Sannolikhet		
1	**Osannolikt**	Det finns få eller inga tecken på att hotet kan inträffa genom de angivna sårbarheterna.
2	**Liten sannolikhet**	Det finns vissa tecken på att hotet kan inträffa genom de angivna sårbarheterna i vissa delar av verksamheten. Inträffar sannolikt inte under normala omständigheter och i vart fall inte frekvent.
3	**Stor sannolikhet**	Det finns tydliga tecken på att hotet kan inträffa genom de angivna sårbarheterna i vissa delar av verksamheten. Kan mycket väl inträffa men troligtvis inte särskilt frekvent.
4	**Mycket stor sannolikhet**	Det är bekräftat att hotet kan inträffa genom de angivna sårbarheterna i väsentliga delar av verksamheten i närtid.

Figur 2 – Skala för sannolikhet.

4.2 Skala för konsekvens

För att fastställa konsekvensen för brister i konfidentialitet, riktighet eller tillgänglighet hos skyddsvärda informationstillgångar ska skalan för konsekvens nedanför användas. Konsekvensbedömning görs utifrån skada på individ, verksamhet, samhällsviktig funktion och organisationens förtroende/ekonomi.

Klass	Konsekvensnivå	Kategori	Konsekvensbeskrivning
0	Försumbar	Individs hälsa, fri- och rättigheter eller integritet	Ingen eller försumbar skada på den personliga integriteten för enskild individ, vare sig avseende fysisk, ekonomisk eller integritetsrelaterad skada.
		Kärnverksamhet	Inga svårigheter för verksamheten att nå målen.
		Egen eller andra samhällsviktiga funktioner	Ingen påverkan på samhällsviktiga funktioner.
		Organisationens förtroende och/eller ekonomi	Ingen eller försumbar påverkan på VGR:s förtroende eller ekonomi. Lite negativ uppmärksamhet.
1	Måttlig	Individs hälsa, fri- och rättigheter eller integritet	Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten men som bör kunna övervinnas trots vissa svårigheter.
		Kärnverksamhet	Inga märkbara större svårigheter för verksamheten att nå målen.
		Egen eller andra samhällsviktiga funktioner	Andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär med endast mindre påverkan.
		Organisationens förtroende och/eller ekonomi	Uppleva lindriga besvär men utan påvisbar ekonomisk eller förtroende påverkan. Enstaka missnöjda individer som uttalar sig i sociala medier, eller en notis i lokalmedia.
2	Betydande	Individs hälsa, fri- och rättigheter eller integritet	Enskilda personer kan uppleva konsekvenser, såsom stora fysiska eller psykiska besvär eller stor ekonomisk påverkan som de bör kunna övervinna även om det måste ske med reella och allvarliga svårigheter (exempelvis obehörig spridning av personuppgifter i stor omfattning).
		Kärnverksamhet	Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).
		Egen eller andra samhällsviktiga funktioner	Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder), samhällsviktiga funktioner i egen eller annan organisation påverkas i liten utsträckning.
		Organisationens förtroende och/eller ekonomi	VGR kan påverkas, risk för stor skada, risk för ekonomisk skada. Minskat förtroende genom nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier.
3	Allvarlig	Individs hälsa, fri- och rättigheter eller integritet	Enskilda personers liv och fysiska eller psykiska hälsa äventyras på ett sätt som är oåterkalleligt eller som inte kan övervinnas av den enskilda eller får mycket stora ekonomiska konsekvenser, (exempelvis genom att känsliga personuppgifter sprids till en stor krets obehöriga, skyddade personuppgifter tillgängliggörs eller enskilda riskerar att drabbas av personlig konkurs.
		Kärnverksamhet	Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.
		Egen eller andra samhällsviktiga funktioner	Samhällsviktiga funktioner i egen eller annan organisation påverkas.
		Organisationens förtroende och/eller ekonomi	VGR förlorar förtroende, mycket stor ekonomisk skada. Minskat förtroende exempelvis genom ihållande drev i rikstäckande medier eller av organiserade grupperingar i sociala medier.
4	Av betydelse för Sveriges säkerhet	Finns indikation att informationstillgångar omfattas av säkerhetsskyddslagen ska dessa analyseras och hanteras enligt särskilda bestämmelser i enlighet riktlinje och rutin för säkerhetsskydd och säkerhetspolisens föreskrifter för säkerhetsskydd.	

Figur 3 – Skala för konsekvens.

4.3 Skala för riskacceptans

När riskvärdering genomförs används nedan skala för att bedöma om risk ska hanteras. Skalan är den av VGR fastställda riskacceptans och utgör ett styrande underlag om risken ska vidare till riskbehandling (undvika, acceptera, eliminera, reducera, överföra, bibehålla).

Regional mall för riskhantering är förinställd för att räkna ut riskvärdet, vilket utgör ett underlag för om risken ska accepteras, övervakas eller hanteras.

Skala för riskacceptans	
Acceptabel nivå	Risker som inte kräver någon åtgärd. Risken har värderats lågt och det har bedömts att den inte medför störningar i organisationen. Risk som kan accepteras men som ska bevakas. Dessa risker kan hanteras i den löpande verksamheten.
Övervakningsnivå	Risker som behöver analyseras djupare. Riskerna ska bevakas i syfte att snabbt kunna sätta in åtgärd om händelsen inträffar.
Oacceptabel nivå	Allvarliga risker som behöver åtgärdas snarast. Riskerna har värderats med hög sannolikhet eller hög konsekvens. Dessa risker kräver åtgärder från ansvarig chef och ska rapporteras till ledningen.

Figur 4 – Skala för riskacceptans.

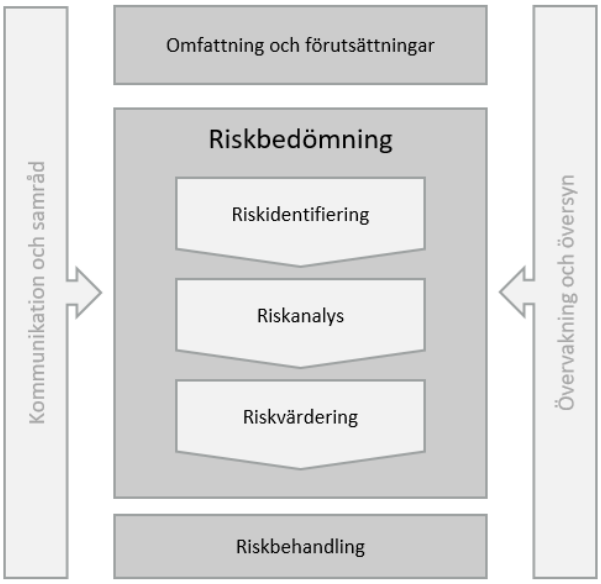
5 Genomförande

Genomförandet av riskhantering består av flera delar och är ett strukturerat sätt att identifiera och värdera informationssäkerhetsrisker inom ett givet analysområde.

Utgångspunkten är att först identifiera potentiella hot som skyddsvärda informationstillgångar kan utsättas för, för att sedan gå vidare och identifiera vilka sårbarheter som hoten kan utnyttja.

Därefter analyseras sannolikheten att hoten blir verklighet och deras potentiella konsekvens för verksamhet och individ. Det ingår även att planera för åtgärder för att behandla risken.

Riskhantering förutsätter ett löpande arbetssätt där det kan finnas behov av att gå tillbaka och komplettera med tillkommande risker och dokumentera genomförda säkerhetsåtgärder.



Figur 5 – Översiktlig bild av riskhanteringsprocessen utifrån SS-ISO/IEC 27005:2022.

5.1 Omfattning och förutsättningar

Tydliggör omfattning av analysen med en kort beskrivning, vilken dokumenteras i regional mall för riskhantering.

Följande underlag kan vara lämpliga att ha med i arbetet och har generellt tagits fram vid arbetet med informationsklassning:

- en beskrivning av omfattning av analysen, de verksamhetsprocesser, aktiviteter eller IS/IT-tjänster som ska inkluderas,
- rättsliga krav som informationstillgångarna omfattas av,

- gränsdragning till vad som ska omfattas och inte omfattas av analysen och motiv för detta,
- eventuell dokumentation av teknisk plattform samt
- resultat från granskningar och relaterade analyser, exempelvis från revisioner, tidigare genomförda riskanalyser eller inträffade incidenter.

5.2 Riskbedömning

Riskbedömningen dokumenteras i regional mall riskhantering för informationssäkerhet och omfattar:

- riskidentifiering,
- riskanalys samt
- riskvärdering.

Riskbedömning bör ha föregåtts av informationsklassning, så att det finns kännedom om vilka informationstillgångar som är skyddsvärda och därmed kan utsättas för risk.

Riskidentifiering

Riskidentifiering innebär identifiering av:

- *Skyddsvärda informationstillgångar*: Information av olika slag som är av värde för organisationen och som utsätts för informationssäkerhetsrisker.
- *Hot*: Möjlig orsak till en oönskad händelse som kan medföra negativa konsekvenser för verksamheten och/eller individ. Det är informationstillgången och dess sårbarhet som utsätts för hot. Hot ska värderas enligt sannolikheten att de inträffar samt konsekvensen det skulle innebära om de inträffar.
- *Sårbarheter*: Brist i skyddet av en informationstillgång som kan utnyttjas av ett eller flera hot.

Resultatet från riskidentifiering är en sammanställning av informationssäkerhetsrisker samt integritetsrisker som skulle kunna äventyra verksamheten att nå informationssäkerhetsmålen.

Riskanalys

Riskanalys handlar om att beskriva de oönskade konsekvenserna för individ/verksamhet i de fall ett hot skulle inträffa.

I riskanalysen bestäms riskvärdet, summan av den troliga sannolikheten och konsekvenserna för verksamhet och integritet. För att bedöma

används skala för sannolikhet och skala för konsekvens (båda under avsnittet Bedömningsmetod).

Resultatet av riskanalysen är en förståelse för riskens karaktär och vad en förlust av informationens konfidentialitet, riktighet eller tillgänglighet skulle kunna få för konsekvenser för organisationen och dess informationssäkerhetsmål.

Riskvärdering

I denna del ingår att värdera riskacceptansen. När värdering genomförs används fastställd skala för riskacceptans för att bedöma om och hur risk ska hanteras. Skalan är styrande för om risken ska tas vidare till riskbehandling.

5.3 Riskbehandling

Riskbehandling är en iterativ process tills risken kan accepteras och dokumenteras i regional mall riskhantering för informationssäkerhet.

Riskbehandling innebär förslag på säkerhetsåtgärder med syfte att:

- undvikande av risk,
- eliminerande risk,
- reducera risk eller,
- accepterande av risk.

Utifrån de åtgärder som föreslås skapas en plan som innehåller åtgärdsbeskrivning, åtgärdsansvarig, riskägare, tidplan och prioritering. Vid riskbehandling ska kostnad för åtgärd övervägas mot kostnaden för eventuellt inträffad händelse.

Avslutningsvis görs en förnyad riskbedömning per risk som visar uppskattad konsekvens och sannolikhet efter föreslagen åtgärd.

Överlämna sedan förslaget på av riskbehandlingen till riskägaren för godkännande. Det är riskägaren som kan fatta beslut om riskbehandling och framförallt om att också acceptera risker. Den som fattar beslutet måste förstå konsekvensen av risken.

Om det finns flera olika riskägare för de risker som identifierats behöver samtliga godkänna.

Riskägaren ansvarar för att följa upp implementationen av beslutade säkerhetsåtgärder.

5.3.1 Kommunikation och samråd

Syftet med kommunikation och samråd inom riskhantering för informationssäkerhet är att säkerställa att riskägaren känner sig ansvarig

för de risker som finns inom dennes verksamhet. Resultatet av riskhanteringen ska kommuniceras till riskägare och berörda intressenter för att möjliggöra ansvarstagande på olika nivåer i verksamheten.

5.3.2 Övervakning och översyn

Syftet med övervakning inom riskhantering för informationssäkerhet är att säkerställa att riskbehandlingen är effektiv och ändamålsenlig.

Övervakning och översyn innebär att analysera och dra lärdomar av incidenter, förändringar, trender, framgångar och andra händelser som kan bidra till att upptäcka framväxande risker.

6 Dokumentation

Arbetet ska dokumenteras i regional mall för riskhantering. Använd med fördel ett digitalt godkännande i diariet när riskägaren fastställer resultatet.

Dokumentationen arkiveras enligt anvisning i myndighetens informationshanteringsplan.

Information som ingår i riskhantering kan vara mycket känslig. Det kan därför vara nödvändigt att begränsa insyn genom att sekretessbelägga handlingen i enlighet med offentlighet- och sekretesslagen.

7 Nästa steg

Informationssäkerhetsrisker av regionövergripande karaktär ska eskaleras av riskägaren till informationsstyrningsrådet.

8 Relaterade dokument och länkar

- Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet
- Riktlinje för informationssäkerhet och dataskydd (RS 2023-02811)
- Informationsstyrningsrådet på intranätet: Informationsstyrningsrådet - Koncernkontoret (vgregion.se)
- Regional mall riskhantering för informationssäkerhet

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-118

Version: 4.0

Giltig från: 2024-08-05

Giltig till: 2028-07-24