VÄSTRA GÖTALANDSREGIONEN

Koncernkontoret
Enhet säkerhet

Dokumenttyp	Övergripande dokument	Version
Rutin	Riktlinjer för informationssäkerhet	1.0
Dokumentansvarig	Kontaktperson	Dnr
Valter Lindström	Monika Göransson	RS 129-2015
Beslutad av	Giltig från	Ersätter
Valter Lindström, koncernsäkerhetschef	2015-11-09	Regional instruktion för riskanalyser inom VGR 2004-02-13

RUTIN FÖR RISKANALYS

Mål

Risker som kan påverka Västra Götalandsregionens informationssäkerhet ska identifieras, analyseras och hanteras.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

Utgångspunkt

Ramverket för säkerhet och perspektiven **före–under–efter** tillämpas såväl för informationssäkerhet som för annat säkerhetsarbete. Tyngdpunkten ligger på det förebyggande arbetet där riskhantering är en grundläggande aktivitet.

Allt säkerhetsarbete utgår från det som är skyddsvärt för VGR och medborgarna.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

1 Omfattning

Anvisningen ska tillämpas för bedömning av informationssäkerhetsrisker oavsett var och i vilken form regionens informationstillgångar hanteras. Den är också lämplig för andra riskanalyser.

2 Beskrivning

Det är viktigt att organisationen känner till, bedömer och hanterar de risker som kan inverka på möjligheten att uppfylla verksamhetens uppdrag och uppsatta mål. Risker ska därför identifieras och analyseras, och ansvariga ska ta ställning till hur riskerna ska hanteras. En viktig del i denna riskhanteringsprocess är riskanalys. Den ska tillämpas inom alla verksamheter och vara en del av beslutsunderlaget inför förändringar. Riskanalysen ska göras i förebyggande syfte och leda till att ett lämpligt val av skyddsåtgärder genomförs i syfte att minska verksamhetens risknivå.

En riskanalys ska genomföras på ett metodiskt och strukturerat sätt, lämpligen i workshopform. Det är av stor vikt att deltagarna känner till det aktuella området väl och att de väljs så att alla nödvändiga riskperspektiv täcks in.

En riskanalys kan kort beskrivas som svaret på tre frågor:
Vad kan hända? Hur sannolikt är det? Vad konsekvensen om det händer?
En sårbarhetsanalys är svaret på varför det kan hända.

Se även bilaga 1: Viktiga begrepp i analysarbetet och illustration av komplexa samband mellan de olika modulerna i en process för riskhantering

Följande steg bör genomföras inom ramen för risk- och sårbarhetsanalysen:

1. Identifiera och säkerställ en beställare av riskanalysen.
2. Definiera analysobjektet (projekt, process, rutin, organisation, system etc.) och dess avgränsning.

   Steg 1 – identifiera skyddsvärda tillgångar och hot
   Steg 2 – riskbedömning
   Steg 3 - riskhantering
3. Överlämna analysen till beställaren för beslut om och genomförande av åtgärder (riskreduktion/kontroll).

Beställaren ansvarar för att följa upp de riskreducerande åtgärderna. Om effekten inte är den önskade, ska beställaren ta ställning till vilka ytterligare skyddsåtgärder som behöver genomföras.

3 Bedömningsmetod

Steget att besluta och fastställa skala för sannolikhet ska genomföras innan analysen påbörjas. Om det inte är gjort innan, kommer diskussioner om bedömningskriterierna och vilka kriterier som ska gälla att uppstå.

Det finns olika metoder och modeller för att genomföra riskanalyser. Analysledaren fastställer vilken skala för sannolikhet som ska användas.

Skala för sannolikhet (alternativ 1)

(Används lämpligen för t ex informationssäkerhet)
När risknivån bedöms kan följande skala användas för att fastställa sannolikheten att ett hot eller en risk ska inträffa. Det är viktigt att identifiera och anpassa analysobjektets livscykel, t.ex. hur ofta en risk eller negativ händelse förväntas inträffa.

Skala för sannolikhet (alternativ 2)

(Används lämpligen för t ex patientsäkerhet)
När risknivån bedöms kan följande skala användas för att fastställa sannolikheten att ett hot eller en risk ska inträffa. Det är viktigt att identifiera och anpassa analysobjektets livscykel, t.ex. hur ofta en risk eller negativ händelse förväntas inträffa.

Sannolikhet		Tabell 1	Tabell 2
1	Osannolikt	Inträffar en en gång per år	Det finns mycket få eller inga tecken på att hotet är verklighet i dag.
2	Liten sannolikhet	Inträffar en gång på per månad	Inträffar sannolikt inte under normala omständigheter och i vart fall inte frekvent. Det finns vissa tecken på att hotet är verklighet i mindre omfattning i dag.
3	Stor sannolikhet	Inträffar en gång per vecka	Kan mycket väl inträffa men troligtvis inte särskilt frekvent. Det finns tydliga tecken på att hotet är verklighet i vissa delar av verksamheten redan i dag.
4	Mycket stor sannolikhet	Inträffar en gång dygn	Sannolikheten är stor att det ska inträffa. Det är bekräftat att hotet är verklighet i väsentliga delar av verksamheten redan i dag eller att den väntas bli det i närtid.

Skala för konsekvens

När risk ska bedömas bör följande skala användas för att fastställa konsekvensen om den in

Konsekvens				
1	Försumbar	Patient/medarbetare	Liten påverkan på liv, hälsa, rättigheter.	Ingen eller obetydlig skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. Ingen eller obetydlig förtroendeskada för verksamheten.
		Process	Liten negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Ingen märkbar skadekostnad för verksamheten.	
2	Lindrig	Patient/medarbetare	Påverkan på liv, hälsa, rättigheter.	Begränsad skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. (Kan hanteras i det löpande arbetet.) Begränsad förtroendeskada för verksamheten.
		Process	Begränsad negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Viss skadekostnad för verksamheten.	
3	Allvarlig	Patient/medarbetare	Stor påverkan på liv, hälsa, rättigheter.	Allvarlig skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. Allvarlig förtroendeskada för verksamheten.
		Process	Stor negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Stor skadekostnad för verksamheten.	
4	Mycket allvarlig	Patient/medarbetare	Mycket stor påverkan på liv, hälsa, rättigheter (skadade eller dödsfall).	Mycket allvarlig skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om den inträffar. Mycket allvarlig förtroendeskada för verksamheten.
		Process	Mycket stor negativ effekt på verksamhetens förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.	
		Ekonomi	Mycket stor skadekostnad för verk-samheten.	

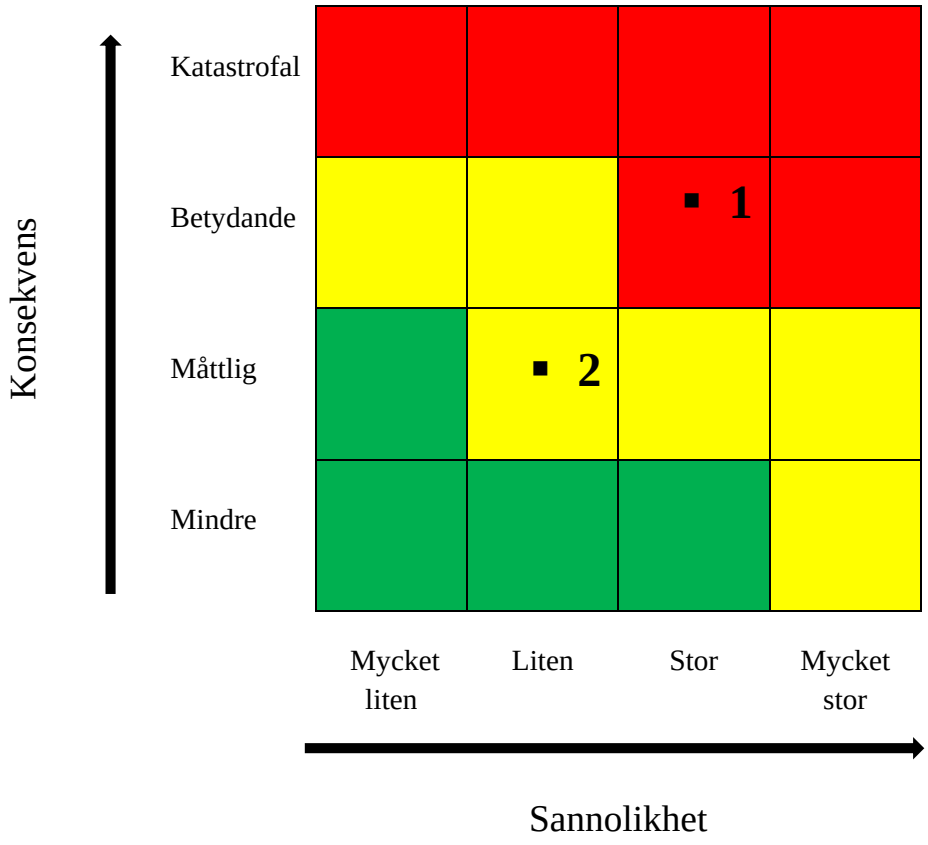
Skala för acceptans

När riskanalys genomförs bör följande skala användas för att bedöma om en risk kan accepteras eller inte.

Kategori	Beskrivning
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.
Övervaknings-nivå	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.

Riskmatris

Riskmatrisen nedan kan användas för att få en grov överblick över de risker som identifierats. Färgerna i riskmatrisen beskriver om en risk är acceptabel eller inte enligt toleransnivåerna, se ovan.



Steg 1 – identifiera skyddsvärda tillgångar och hot

Frågan som ska ställas är ”Vad ska analyseras?” och ”Vilka skyddsvärda tillgångar ingår i analysen?”

Skyddsvärda tillgångar kan vara ett IT-system, information, personal, byggnader, en process. När skyddsvärda tillgångar identifierats och dokumenterats är det dags att identifiera händelser som kan hota det skyddsvärda. Dessa hot dokumenteras i kolumn ”Hot”.

Steg 1 - Identifiera skyddsvärda tillgångar och hot			
Skyddsvärt		Hot	
ID	*Beskrivning*	*ID*	*Hot*
		H01	
		H02	
		H03	
		H04	
		H05	
		H06	
		H07	
		H08	
		H09	
		H10	

Steg 2 - riskbedömning

Hjälptabellen nedan kan användas för att få fram den sammanvägda risknivån för respektive risk. Exemplet nedan visar två identifierade risker, de nivåer som bedömts för sannolikhet och konsekvens samt risknivåerna.

Steg 2 - Riskbedömning				
Konsekvensbeskrivning Vilka blir konsekvenserna om hotet inträffar.	Riskbedömning innan åtgärd			Fortsatt analys?
Beskrivning av konsekvensen	Konsekvens	Sannolikhet	Riskvärde	

Steg 3 - riskhantering

Riskhantering ska genomföras genom att sårbarheten identifieras och förslag på åtgärd, ägare och tidplan tas fram och dokumenteras. Avslutningsvis görs en riskbedömning av sannolikhet och konsekvens om hotet inträffa efter genomförd skyddsåtgärd.

Steg 3 - Riskhantering							
Sårbarheter Vilka problem/brister ligger bakom riskerna?	**Åtgärdsförslag** Vad kan göras för att eliminera, begränsa eller bevaka riskerna och dess sårbarheter?	**Ansvarig för åtgärd** Vem/vilka ansvarar för åtgärderna?	**Ägare hot** Vem äger hotet och har övergripande ansvar för att åtgärderna genomförs?	**Tidplan** När ska åtgärden vara genomförd?	**Riskbedömning efter åtgärd**		
					Konsekvens	**Sannolikhet**	**Riskvärde**

Skyddsåtgärder ska vidtas för att kontrollera och reducera risker som identifierats vid riskanalyser. En viktig kontrollfråga vid val av skyddsåtgärder är om föreslagna åtgärder förändrar bedömningen av risknivå (sannolikhet och konsekvens). Målet är att riskerna efter vidtagna skyddsåtgärder ska ligga på en acceptabel nivå.

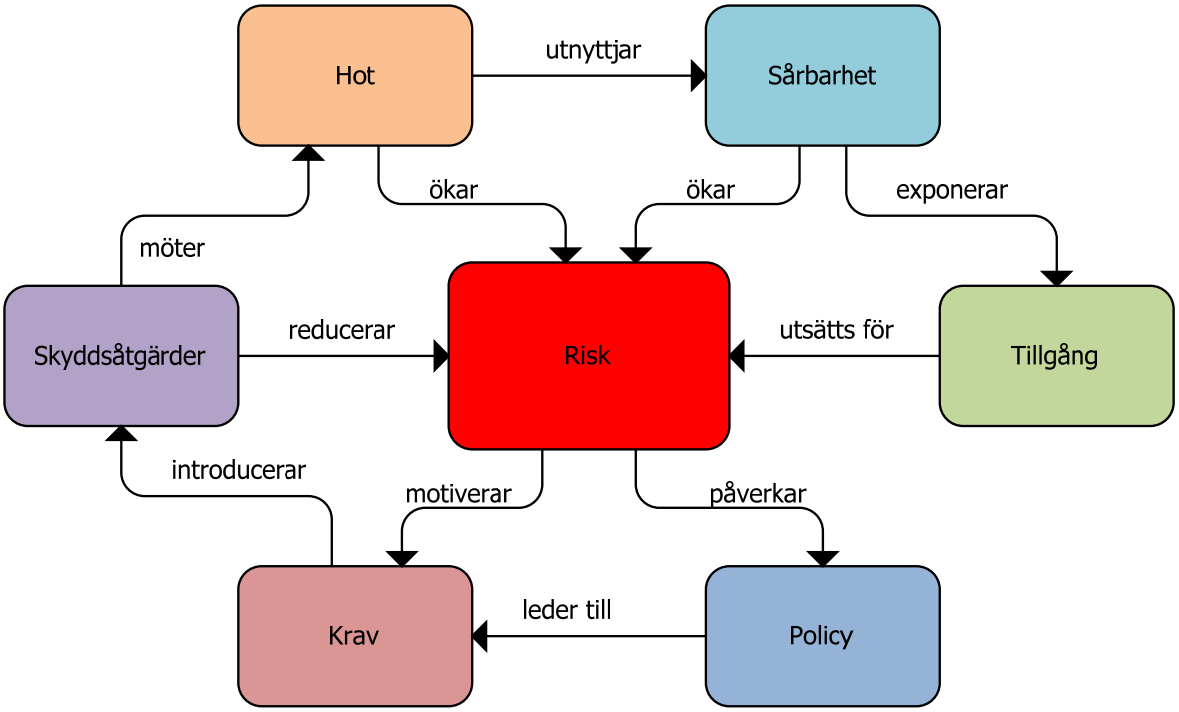
Den som fattar beslutet måste också väga kostnaden för skyddsåtgärden mot kostnaden för eventuellt inträffad händelse och besluta i vilka fall det inte är relevant att vidta åtgärder, då det medför en högre kostnad än vad som kan motiveras utifrån konsekvens och kostnad för inträffad händelse.

Bedömning av vad som är en acceptabel nivå ska göras utifrån

- verksamhetens interna krav
- lagstiftning och andra externa krav
- kostnaden för att vidta skyddsåtgärder jämfört med kostnaden om risken förverkligas

4 Beskrivning av samband i process för riskhantering

Bilden nedan visar på de komplexa sambanden mellan olika moduler i en process för riskhantering och hur de påverkar varandra.



5 Termer

Hot	Möjlig, oönskadhändelse med negativa konsekvenser för organisationen
Konsekvens	Resultat av en händelse med negativ inverkan. Kan vara ekonomisk, dåligt anseende eller t ex legal påverkan
Sannolikhet	Ett mått på hur troligt det är att ett hot realiseras
Risk	Produkten av sannolikhet och konsekvens för att ett hot realiseras
Riskhantering	Samordnade aktiviteter för att leda och styra en organisation med avseende på risk
Sårbarhet	Bristande förmåga hos en organisation, en process eller ett IT-system, att motstå och återhämta sig från olika former av påfrestningar.