4 RISKHANTERING

4.1 Mål

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

4.2 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.

4.3 Riskhantering

Riskhantering är samordnade aktiviteter för att leda och styra en organisation med avseende på risk. Riskhanteringsprocessen i Västra Götalandsregionen är en generisk modell, som ska tillämpas av varje verksamhet och vara en del av beslutsunderlaget inför förändringar.

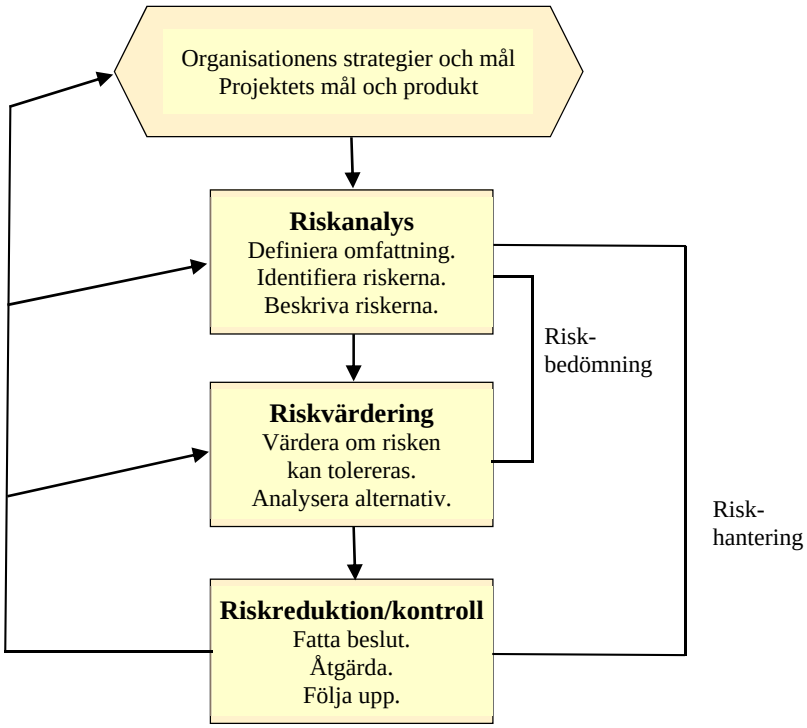

Bild 5: Schematisk bild av riskhantering

För genomförande av riskanalys se *VGR-rutin för riskanalys*.

Riskhantering ska som minimum genomföras vid:

- Etablering av nya IS/IT-system
- Organisations-/processförändringar som kan påverka informationsbehandlingen
- Tekniska förändringar i infrastruktur eller programvaror, som kan påverka informationsbehandlingen
- Om molntjänster eller outsourcing av funktioner eller IS/IT-tjänst övervägs.

4.3.1 Uppföljning

För att kontrollera om effekten är den önskade ska genomförda aktiviteter och fattade beslut dokumenteras och följas upp.

4.4 Ansvar

Ansvaret för riskhanteringen följer linjen, vilket innebär att respektive förvaltning ska integrera riskhanteringsprocessen och dess aktiviteter i det egna ledningssystemet. Det ska tydligt framgå i vilka forum som beslut om åtgärder fattas.

I regionens styr- och förvaltningsmodell för IS/IT ansvarar respektive informations- och resursägare för att riskhanteringsprocessen genomförs, i samverkan med berörda verksamheter. Samma beslutsvägar tillämpas som för övriga objektbeslut.

4.5 Eskalering av hot och risker av regiongemensam karaktär

Hot och risker som inte kan hanteras i linjen eller inom VGR:s styr- och förvaltningsmodell för IS/IT ska eskaleras till koncernsäkerhetschefen, för beredning i det regionala riskhanteringsrådet och därefter beslut av regiondirektör alternativt beslut i lämplig politisk församling.