Rev 31-2008

Västra Götalandsregionen

Rapport: Styrning av VGRnet

Göteborg, 2009-02-03

ERNST & YOUNG

Sammanfattning

Bakgrund

Ernst & Young har fått i uppdrag av Västra Götalandsregionens revisionsenhet att göra en granskning av styrningen av regionens IT-verksamhet.

Syftet med granskningen är utvärdera om styrningen av IT-verksamheten, inklusive riskhanteringen, är ändamålsenlig. Granskningen har avgränsats till förhållanden kring regionens gemensamma nätverk VGRnet och omständigheter som berör hälso- och sjukvården.

Bakgrunden till granskningen är bl.a. de två senaste årens förändringar av regionens IT-organisation samt två IT-incidenter relaterade till VGRnet, som inträffade under våren 2008.

Granskningen har gjorts dels mot iakttagelser i tidigare revisionsrapporter, dels mot rekommendationer i COBIT. COBIT är ett för sammanhanget relevant och etablerat ramverk som utgör ledande praxis för styrning och organisation av IT inom en verksamhet.

Iakttagelser

Regionens IT-organisation har genomgått stora förändringar under de senaste två åren. Fram till 2007 har flertalet av regionens förvaltningar och bolag bedrivit sin IT-verksamhet med egna IT-organisationer, som ansvarat för drift, support, förvaltning, strategi och utveckling. Mindre förvaltningar har anlitat den interna leverantören IT-centrum för flera av dessa tjänster. IT-Centrum har dessutom tillhandahållit drift- och supporttjänster för regiongemensamma system och utvecklingsprojekt.

Efter förstudier genomfördes ett konsolideringsprojekt av regionens IT-funktioner och resurser, med syfte att utveckla ett mer regiongemensamt perspektiv. Ett led i konsolideringen var bildandet av VGR IT, den 1 januari 2007. VGR IT är idag en av regionens interna serviceorganisationer som ingår i Regionservice under Servicenämnden. Sedan bildandet av VGR IT har organisationen successivt utvecklats och ansvarsområden utformats. Den senaste förändringen som innebar en omorganisation av enheten Infrastruktur inom VGR IT beslutades så sent som den 1 november 2008 och tillsättandet av nya rollinnehavare pågick under tiden denna granskning genomfördes.

I samband med att VGR centraliserat flera av verksamheternas IT-funktioner har beställarorganisationen förändrats och således har även styrningen av VGRnet påverkats. En del förvaltningar upplever att regionens nya organisation fungerar på pappret, men att den hittills ännu inte har förankrats i verksamheten tillräckligt. Vissa intressenter uttrycker också missnöje med att det är långa beslutsvägar och råder brist på kostnadsuppföljning. Det framkommer även att de strategiska handlingsplaner för utveckling av VGRnet som är framtagna under hösten 2008 inte är kända, hos personer som kan förväntas vara informerade. Detta utvecklas närmare i rapporten.

Trots en del kritik, främst kring styrningen av VGRnet, framgår det tydligt att uppfattningen hos både *beställarna* IT-strategiska avdelningen (ITSA), *nyttjarna* förvaltningar och bolag samt *utförarna VGR IT,* att VGRnet är ett nät med bra prestanda, hög stabilitet och hög säkerhet. Antalet incidenter har också varit få under de senaste fem åren.

Rapporten har ett fokus på att framhålla förbättringsområden. I det sammannhanget är det väsentligt att notera att organisation och rutiner kring infrastrukturen och i synnerhet VGRnet, genomgår förändringar under pågående granskning. Flera av förbättringsområdena som tas upp finns redan på agendan, men vi väljer att påtala dem, för att minska risken att de senare blir nedprioriterade.

Väsentliga förbättringsområden

I denna sammanfattning redovisas de områden som vi bedömer är mest väsentliga att förbättra. I avsnitt fyra (4) redovisas våra iakttagelser mer detaljerat i prioriteringsordning, tillsammans med våra rekommendationer.

- Beställar-/utförarmodellen är inte fullt implementerad. Det finns inget renodlat forum för beställarna, utan utföraren VGR IT deltar i alla forum. De intervjuade visar också att det råder en otydlighet kring den nya organisationen som utformats genom projektet BestIT under 2007. Det som är beskrivet i dokument är inte realiserat i praktiken. Det gäller otydligheter om vilka funktioner som ansvarar för vad, vilka beslut och vilka mandat som gäller o.s.v. För flertalet av respondenterna är det t.ex. oklart vem som är systemägare av VGRnet. Sannolikt bottnar denna otydlighet i att den nya organisationen inte satt sig ännu och att den delvis är bristfälligt kommunicerad.
- VGR IT har hittills endast haft begränsad uppföljning av kostnaderna för förvaltning och utveckling av VGRnet. När IT-resurserna sammanfördes i VGR IT lades alla tidigare IT-kostnader i en gemensam ”pott”, där de sedan fördelades för att interndebiteras förvaltningarna med 1/12 per månad. Det finns i nuläget ingen redovisning vad olika IT-tjänster, bl.a. VGRnet kostar en förvaltning. En prissatt tjänstekatalog håller på att tas fram.
- Innehållet i och omfattningen av avtal för lokala nätverk mellan VGR IT och förvaltningarna varierar. Förvaltningarna efterfrågar särskilt servicenivåavtal för att veta vad de kan förvänta sig av VGR IT.
- I avtalet mellan ITSA och VGR IT är tillgängligheten till kärnnätet reglerat till minst 99,81%. Incidenter följs upp men det sker ingen formell uppföljning av den faktiska tillgängligheten. Rapporterings- och eskaleringsvägar i samband med IT-incidenter fungerar inte sedan omorganisationen med VGR IT genomfördes.
- Fullständiga kontinuitetsplaner existerar ej för samtliga förvaltningar och det sker endast en begränsad uppföljning av att riskanalyser och efterlevanden av kontinuitetsplanering.
- Beslutsvägarna för investeringar uppfattas som otydliga och investeringsprocessen upplevs som inkonsekvent och ineffektiv.
- Nuvarande investeringsmodell gör också att VGR IT kan gå direkt till regiondirektören med en investering utan att behandla ärendet tillsammans med ITSA och förvaltningar i RegSam och IT-rådet.
- För varje investering skall en investeringsbudget tas fram. Det framhålls att det är oklara krav på hemtagande i investeringsbudgetar samt att de kostnads-/nyttoanalyser som genomförs är av undermålig kvalitet.

Innehållsförteckning

Sammanfattning **2**

1 Bakgrund **5**

1.1 Inledning 5
1.2 Syfte 5
1.3 Avgränsningar 5
1.4 Metod 5

2 Iakttagelser **8**

2.1 Vad är VGRnet? 8
2.2 IT-organisation och IT-verksamhet 8
2.3 Strategier 13
2.4 Teknisk inriktning 14
2.5 Avtal 14
2.6 Investeringar och kostnader 15
2.7 Säkerhet och riskhantering 16
2.8 Projekthantering 19

3 Slutsatser och rekommendationer **20**

3.1 Generella slutsatser 20
3.2 Rekommendationer 20

Bilaga Granskningsprogram ur COBIT **24**

1 Bakgrund

1.1 Inledning

Ernst & Young har fått i uppdrag av revisorerna vid Västra Götalandsregionen (VGR) att göra en granskning av styrningen av regionens gemensamma nätverk - VGRnet. VGRnet används för all transmission av data och en stor del av den fasta telefonin mellan regionens enheter såväl med omvärlden. VGRnet är ett av nordens största och mest komplexa nätverk och utgör därigenom en ytterst kritisk komponent för en stor del av regionens informationsbehandling.

Bakgrunden till granskningen är bl.a. de förändringar i regionens IT-organisation som genomförts under de senaste åren, samt två IT-incidenter relaterade till VGRnet:

- De senaste åren har regionens **IT-organisation förändrats** och utvecklats. Den 1 januari 2007 bildades VGR IT som ett led i en omfattande konsolidering av flera av förvaltningarnas och bolagens IT-funktioner och IT-resurser. Bildandet av VGR IT innebar att IT-driftorganisationerna samlades för att samordnas under Regionservice. Ansvaret för telefoni (teknik) sammanfördes också till VGR-IT. Detta betyder att regionen numer i princip har infört ett beställar-/utförarsystem för IT-verksamheten. Den IT-strategiska avdelningen (ITSA) inom regionstyrelsens kansli är företrädare för regionledningen. ITSA är beställare (och i vissa avseenden ägare), nämnder och förvaltare är nyttjare och VGR IT är utförare.
- I april 2008 drabbades regionen av **två IT-incidenter** som påverkade tillgängligheten till telefoni och IT. Händelserna har analyserats och en rapport har redovisats för regionstyrelsen. Regiondirektören har därefter expedierat rapporten till förvaltningscheferna, regionkansliets informationsavdelning och VGR IT med uppdrag att förbättra och stärka regionens förmåga att hantera liknande händelser i framtiden.

1.2 Syfte

Granskningens syfte är att **utvärdera om styrningen av VGRnet är ändamålsenlig**, inklusive organisation, roller, ansvar och risk- och incidenthantering.

1.3 Avgränsningar

För att begränsa granskningen håller vi oss på en principiell nivå. Granskningen är problematiserad utifrån de refererade incidenterna och avgränsad till omständigheter som berör hälso- och sjukvården och till följande förvaltningar och enheter:

- IT-strategiska avdelningen
- VGR-IT
- Primärvården i Göteborgsområdet
- Tandvården i Fyrbodal
- Regionens Hus i Vänerborg och Lillhagsparken
- NU-sjukvården

1.4 Metod

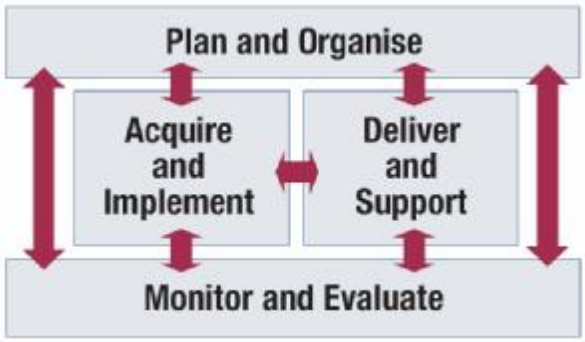
Uppdraget har genomförts genom informationsinsamling och analys av de omständigheter som råder under hösten 2008 i förhållande till ledande praxis i enlighet med ramverket CobiT 4.1.

Granskningen har genomförts som en dokumentstudie tillsammans med intervjuer av nyckelpersoner som representerar olika intressenter inom regionen.

1.4.1 CobiT

COBIT (Control Objectives for Information and Related Technology) är ett ramverk för IT-styrning som utfärdats av IT Governance Institute (ITGI). Genom COBIT definieras de generiska processer som generellt krävs för att IT skall uppfylla för att stödja en organisations verksamhetsmål.

Ramverket är strukturerat i fyra domäner, se bild nedan:



I granskningen har den senaste versionen av ramverket använts, och då denna granskning är begränsad till styrning och riskhantering av VGRnet har följande processer ur COBIT valts ut ur domänen Plan and Organise (PO):

- PO1: IT-strategi
- PO3: Teknisk inriktning
- PO4: IT-organisation
- PO5: Investeringar
- PO9: Riskhantering
- PO10: Hantera projekt

Mer information om COBIT finns på www.isaca.org/cobit.

1.4.2 Dokumentation

Följande dokument har studerats:

[1] *Enheten Infrastruktur, Organisation och arbetssätt*, 2008-11-04

[2] *Regionperspektiv och samverkan i Västra Götalandsregionens IT-verksamhet*, 2005-08-31

[3] *Förslag funktionsområdesstruktur*, 2008-03-19

[4] *Beslut beställarmodell IS/IT*, 2007-03-30

[5] *Rapport, IT-incidenter den 7 april*, 2008-05-08

[6] *IT-infrastruktur strategi VGRnet*, 2004

[7] *Ramverk och riktlinjer för säkerhetsarbetet*, 2008-03-11

[8] *Policy för säkerhetsarbete i Västra Götalandsregionen*, 2008-02-11

[9] *Regional anvisning för styrning av kommunikation och drift v1.0* (ej daterad)

[10] *Beskrivning av regiongemensamma IT-tjänster*, 2005-09-23

[11] *Regional anvisning för kontinuitetsplanering v1.1* (ej daterad)

1.4.3 Intervjuer

Intervjuer har genomförts med medarbetare hos ITSA, VGR-IT samt utvalda nämnder och förvaltningar inom regionen. Urvalet av intervjupersoner har gjorts av Ernst & Young tillsammans med revisorerna för VGR. Följande personer har intervjuats:

- *Hans Ekman*, IT-direktör, ITSA
- *Mikael Johansson*, Funktionsområdesansvarig Infrastruktur, ITSA
- *Mats Gustavsson,* Inköpscontroller och kundansvarig mot förvaltningar, VGR IT
- *Diana Olausson Öberg*, Enhetschef Infrastruktur, VGR-IT
- *Leif Ytterström*, Chef för sektionen Kommunikation inom VGR-IT Infrastruktur
- *Bent Petersen*, utvecklingschef, Folktandvården
- *Thomas Stegberg*, IT-strateg, NU-sjukvården
- *Bodil Warolin,* kanslidirektör, Regionens Hus
- *Hans Lilja,* administrativ utvecklingschef, Primärvården
- *Valter Lindström,* Säkerhetsdirektör, Regionens hus

Utredarna vill i sammanhanget framföra ett tack till alla de personer som på ett öppet och konstruktivt sätt delat med sig av sina erfarenheter och åsikter vid de intervjuer vi gjort.

2 Iakttagelser

2.1 Vad är VGRnet?

Enligt definition så är VGRnet det regiongemensamma kommunikationsnätet som används för utbyte av all elektronisk information, dvs. både data- och telekommunikation.

VGRnet har sin bakgrund ur den kommunikationsstrategi som togs fram 1998 när Västra Götalandsregionen bildades. VGRnet består av ett kärnnät med fyra huvudnoder som sammankopplar Göteborg, Vänersborg, Skövde och Borås. Genom dessa huvudnoder är cirka 700 lokationer inom Västra Götalandsregionen sammankopplade med varandra och omvärlden. Endast bolag och verksamheter ägda till minst 50 % av Västra Götalandsregionen är anslutna till nätet. All kommunikation över nätet är standardiserad och sker med protokollet IP (Internet Protocol en s.k. de-facto-standard för nästan all typ av kommunikation mellan datorer).

VGRnet har från början definierats som en infrastruktur fram till överlämningspunkterna hos förvaltningarna. Av intervjuerna i granskningen framgår att denna avgränsning håller på att lösas upp. Medan några respondenter talar om en strikt uppdelning mellan VGRnet och lokala nätverk, så uppger flertalet respondenter i granskningen att de inte gör någon större åtskiljnad mellan VGRnet och de lokala nätverken. Istället betraktas kommunikationstjänsten och t.o.m. de tjänster som näten bär som en helhet, ända fram till vägguttaget. Detta är troligen en naturlig följ av att det numer inte finns en lokal IT-organisation som ansvarar för det lokala nätverket, istället är det idag enklare när VGR IT ansvarar för helheten.

Fortfarande återstår en del komplexitet i ansvarsfrågorna. Fastighetsnäten ägs ofta av Västfastigheter eller externa fastighetsägare. Det finns en osäkerhet, beroende på vem som är hyresvärd, var ansvaret för nätverken är placerat. Det finns ännu inte heller någon tjänstekatalog eller något servicenivåavtal som definierar VGR IT:s åtagande. Det pågår arbete med att utforma dessa dokument, men fram till att dessa finns, föreligger en otydlighet vilka parter som har ansvar för vad och hur långt ansvaret sträcker sig.

2.2 IT-organisation och IT-verksamhet

2.2.1 En ny IT-organisation

VGR har delat upp sin IT-verksamhet i två organisationer:

- **Beställare** (IT-strategiska enheten)
- **Utförare** (VGR IT)

Utöver dessa två organisationer finns:

- **Nyttjare** (VGR:s bolag och förvaltningar)

Nyttjarna har i regel bara en begränsad egen strategisk IT-funktion kvar. Denne ansvarar för förvaltningens avrop av IT-tjänster av VGR IT. När det gäller nya tjänster eller kravställning är avsikten att dessa behov skall samlas ihop och hanteras under ledning av IT-strategiska enheten.

2.2.2 Beställarfunktioner

Den modell som tillämpas inom regionen modell för beställning av IS/IT-tjänster (BestIT[1]) beslutades av det regionala IT-rådet den 30 mars 2007. Därefter har ansvarsfördelning och rollbeskrivningar utvecklats vidare med motsvarande beredning och beslutsprocess. Viktiga aktörer i denna process är:

IT-strategiska avdelningen (ITSA)
IT-strategiska avdelningen leds av regionens IT-direktör och arbetet utgår från Västra Götalandsregionens IT-vision som beslutades 1999 och reviderades 2006.

IT-direktören betonar att ITSA främst har en uppgift att samordna förvaltningarnas IT-frågor. Enligt ett beslut om ansvarsindelning i det regionala IT-rådet den 4 april 2008 har ITSA också uppgift att vara en beställarfunktion för utveckling och förvaltning av gemensam IT-miljö. Detta ansvar indelas i tre funktionsområden:

- Vård
- Administration
- Infrastruktur.

Funktionsområdesansvar
För respektive funktionsområde finns en Funktionsområdesansvarig (FoA) som ansvarar för att samordna utvecklingen inom funktionsområdet, samt för beställningen av den gemensamma driften och förvaltningen. FoA ansvarar också för att bereda den regiongemensamma budget som fastställs i den årliga budgeten.

Ansvaret för VGRnet tillhör funktionsområdet Infrastruktur.

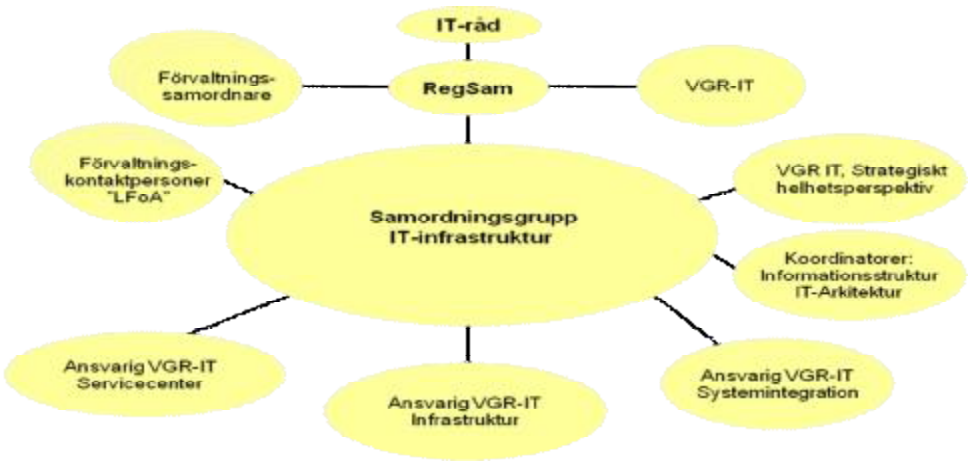
FoA Infrastruktur är sammankallande för en *Funktionssamordningsgrupp*. Detta forum har som syfte att säkra delaktighet och beredning kring utveckling och förvaltning av gemensam infrastruktur. Förvaltningarnas representanter i Funktionssamordningsgruppen går under benämningen *lokal funktionssamordningsansvarig (LFoA)*. Även VGR IT är representerade. Funktionssamordningsgruppen är nyligen bildad och håller på att forma sitt arbetssätt för att fullgöra sina uppdrag. Uppfattningen är att gruppen skall svara för en strategisk, snarare än teknisk utveckling. Avsikten är att samlas till regelbundna möten med en till två månaders mellanrum.

I sammanhanget är det värt att nämna att våra intervjuer har visat att det förekommer en rad olika uppfattningar om ägarskapet för VGRnet, där nämns både IT-direktören, FoA Infrastruktur, VGR IT, IT-rådet och Regiondirektören som tänkbara kandidater. En förklaring till detta är troligtvis att ägarskapet (enligt olika styrande dokument) flyttats mellan olika roller. Det senaste beslutade dokumentet *Förslag struktur funktionsområden 2008-03-27* (med efterföljande godkännande av förslag 2008-04-04) anger dock att det är FoA Infrastruktur som numer är ägare till VGRnet. En frå-

[1] [1] BestIT är ett avslutat internt projekt (2007) med syftet att utforma och beskriva en beställarprocess som tar sin utgångspunkt från verksamhetens behov av styrning av sitt IT-stöd.

ga som är relevant att ställa i sammanhanget är om FoA verkligen har det mandat som rollen systemägare förknippas med.

Regionala Samordningsgruppen (RegSam)
Förslag som har beretts i Funktionssamordningsgrupperna behandlas i den Regionala Samordningsgruppen (RegSam), se bild nedan. RegSam består av IT-direktören, de tre funktionsområdesansvariga representanter för förvaltningarna samt VGR IT. RegSam har en uppgift att samordna och ansvara för beredning av beslutsunderlag. De prioriterar mellan förslag och beslutar hur och av vem beredning skall ske, d.v.s. vilka förstudier som skall genomföras, vilka beslutsunderlag och årsplaner som skall tas fram. RegSam rapporterar till IT-rådet.

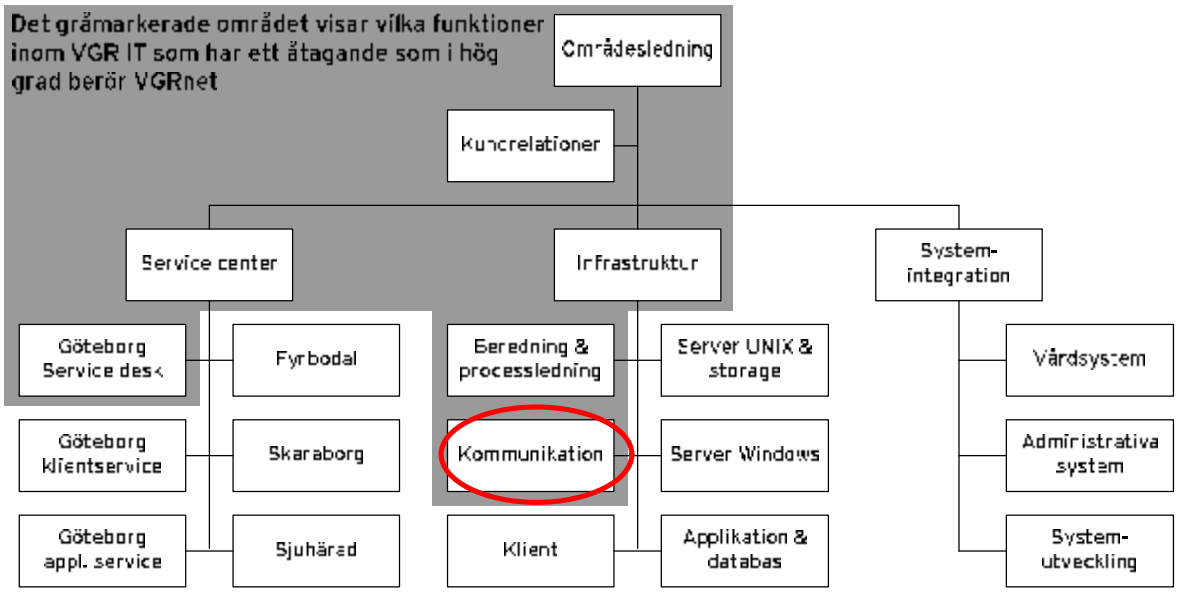


Regionala IT-rådet
IT-rådet har den yttersta beslutsrätten för IS/IT-utvecklingen utom i de fall då besluten skall lyftas till regiondirektör eller regionstyrelse/regionfullmäktige. IT-rådet fastställer årlig driftsbudget för Infrastruktur och beslutar även om en del av de nyinvesteringar som görs i VGRnet. IT-rådet är bemannat med IT-direktören, förvaltningschefer, Ekonomidirektör, personaldirektör samt Direktören för Regionservice och IT-chefen för VGR IT.

2.2.3 Utförare

VGR IT skapades 1 januari, 2007 med syfte att utveckla ett mer regiongemensamt perspektiv på IT. Personal till VGR IT sammanfördes från förvaltningar främst inom sjukvård, primärvård, tandvård samt IT-Centrum. Under 2007 och 2008 har ytterligare omorganisationer genomförts i syfte att skapa gemensam företagskultur och gemensam IT-infrastruktur.

Organisationsschema för VGR IT visas nedan.



Enheten **Service center** inom VGR IT ansvarar för first line support av VGRnet.

Enheten **Infrastruktur** inom VGR IT ansvarar för teknisk design/arkitektur, utveckling och drift av olika infrastrukturprodukter och tjänster till kunder inom Västra Götalandsregionen. Avdelningen Kommunikation har VGRnet som särskilt ansvarsområde.

Enheten **Systemintegration** har inget direkt ansvar kopplat till VGRnet.

2.2.4 Enheten Infrastruktur ansvarar för VGRnet

Enheten Infrastruktur har successivt och egentligen först under andra halvåret 2008 funnit sin organisationsform. Enhetschefen tillsattes så sent som april 2008 och har därefter genomfört förändringar som inneburit att det numer är en tydligare indelning av ansvarsområden och roller.

Enheten Infrastruktur är indelad i sex avdelningar, med ansvar för olika teknikområden. Verksamheten finns beskriven i dokumentet *VGR IT, Enheten Infrastruktur – organisation och arbetssätt, v1.0, 2008-11-04*. Dokumentet beskriver organisationen, styrmodell, ekonomi och investeringar samt mötesformer. Vidare innehåller dokumentet beskrivningar för enhetens olika befattningar och roller. Arbetet med att ta fram och förankra nya befattningar och roller pågick fortfarande i samband med vår revision. Enligt uppgift har de sista rollbeskrivningarna färdigställts under januari 2009. Bemanningsbehov och behovet av att köpa in tjänster skall ses över årligen i samband med budgetarbetet.

Ett annat prioriterat område för enheten Infrastruktur är att se över rutiner och arbetssätt. Målsättningen är att införa ett processorienterat arbetssätt baserat på ITIL (etablerat brittiskt ramverk för support, drift och förvaltning av IT).

Enheten Infrastruktur har identifierat att de har problem med nyckelpersonberoende och har planerat att ta fram handlingsplaner för att möta denna risk. De nyckelpersoner som har identifierats är främst tekniskspecialister. Nyckelpersonsberoendet har vid intervjuerna även påtalats av andra befattningshavare.

En genomgående uppfattning hos flertalet intervjuade är att den teoretiska modell som föreslogs genom projektet BestIT i flera avseende är bra, men inte har blivit implementerad i alla delar och att styrmodellen inte heller fungerar riktigt som det var tänkt. Exempelvis tycks det som förvaltningarna i flera fall för en dialog om behov och utveckling direkt med VGR IT, snarare än att frågor samlas upp och samordnas genom ITSA och FoA Infrastruktur. Det framgår också av intervjuerna att styrmodellen inte är tillräckligt kommunicerad, de beskrivningar som ges om olika aktörers uppdrag varierar i hög grad och uppfattningen är att beslutsgången för investeringar är otydlig.

VGR IT får en del kritik från förvaltningarna, kanske inte direkt riktat mot VGRnet utan snarare mot supporten och att VGR IT:s resurser upplevs vara överbelastade med mindre frågor och att de har svårare att hinna med strategiska frågor. I viss grad har troligtvis det interna arbetet med VGR IT:s organisation och arbetssätt bidragit till detta.

Väsentliga brister:

- I regionens nuvarande modell för beställning av IT-tjänster finns det inget renodlat forum för beställarna, eftersom VGR IT deltar både i FoA Infrastruktur, RegSam och IT-rådet. Det innebär att beställar-/utförarmodellen inte är fullt implementerad.

  En tydligare uppdelning mellan beställare och utförare förutsätter dock att beställarna förfogar över tillräcklig beställarkompetens, inklusive teknisk kompetens.
- Modellens beredning- och beslutsvägar uppfattas som ineffektiva av företrädarna för förvaltningarna.
- Det råder okunskap om ägarförhållanden kring VGRnet.

- Det återstår arbete med att identifiera och planera för nyckelpersonsberoende inom VGR IT.
- VGR IT:s resurser upplevs vara överbelastade med mindre frågor och att de har svårare att hinna med strategiska frågor.

2.3 Strategier

Det finns en formell kommunikationsstrategi som är uppdaterad 2004. Följande är ett utdrag ur kommunikationsstrategin:

”För att kunna möta de mål och krav som finns uppställda inom Västra Götalandsregionens IT Vision, Mål och Strategi skall det finnas ett kraftfullt elektroniskt kommunikationsnät för data, tal och bild som utgör basen för kommunikation i regionen. För att uppnå dessa mål så krävs en utvecklad IT-infrastruktur med ett gemensamt nätverk som plattform ger det stöd som krävs för att regionens och kommunernas verksamheter skall kunna utvecklas.

Tre strategiska mål, ur kund-, process- och ekonomiperspektiv, har fastställts i kommunikationsstrategin. För det första skall VGRnet

1. *Ge bästa nytta för verksamheternas behov*
2. *Målen skall nås genom samverkan och säker kommunikation*
3. *Kostnadseffektivitet inom givna ramar.”*

Flera av de intervjuade indikerar att det råder en oklarhet om vem som har ansvaret att driva strategiska utvecklingsfrågor som omfattar VGRnet. VGR IT har under hösten 2008 tagit fram en regional handlingsplan där flera föreslagna aktiviteter har direkt beröring med VGRnet. Planen har behandlats i tur och ordning av FOA Infrastruktur och Regsam. Planen inkluderar bl.a.:

- Telestrategi och gemensam telefoniplattform.
- VGRnet/LAN strategi
- Utvecklingsprojekt av Quality of Services (QoS) med bl.a. prioritering av nättrafik.
- Gästaccess via nätverket, Private Key Infrastructure (PKI) och Single Sign On (SSO).
- IT-säkerhet, bl.a. säkerhetsöversyn av datorhallar.

En uppfattning intervjuerna ger är att VGR IT hittills har tagit mer initiativ vad beträffar utveckling av VGRnet, medan FoA Infrastruktur har ägnat mer tid åt att formera sig och reda ut sitt uppdrag och arbetssätt. Sannolikheten är stor att denna rollindelning kvarstår genom att den tidigare förvaltaren av VGRnet och därmed en stor del av den tekniska kompetensen har övergått från ITSA till VGR IT.

Väsentliga brister:

- Kommunikationsstrategin har ej uppdaterats sedan 2004, trots större omorganisation av IT-verksamheten och förändrade krav.

2.4 Teknisk inriktning

Analyser om val av teknik, plattformar och arkitektur görs delvis inom olika grupperingar, t.ex. FoA-gruppen, IT-rådet eller inom VGR IT via Teknikområdesansvarig (TA).

Teknikområdesansvarig (TA) på VGR IT är tekniskt ansvarig för teknikteam med regional styrning och utveckling inom teknikområdet, samt medverkar vid investeringar och i arkitektur/designteam. TA bevakar även möjligheter inom teknisk utveckling av infrastruktur.

Bevakning av ny lagstiftning som kan ha inverkan på infrastruktur sker via dagstidningar och nyheterna. Det finns även representanter från VGR IT som sitter i ett nationellt råd där ny lagstiftning presenteras.

VGR IT har nyligen påbörjat arbetet med att ta fram en infrastrukturplan. D.v.s. en plan för val av tekniska lösningar, transmission, säkerhetsnivåer, utbyggnad o.s.v.

Beträffande förändringar i IT-miljön så har VGR IT för avsikt att använda standardiserade processer enligt ITIL Change management process för alla typer av förändringar som skall genomföras. Detta innebär också att alla förändringar på sikt först skall godkännas i ett s.k. Change Advisory Board.

Väsentliga brister:

- **En Aktuell infrastrukturplan saknas.**

2.5 Avtal

Det interna avtalet mellan beställare (ITSA) och utförare (VGR IT) finns reglerat i *Beskrivning av regiongemensamma IT-tjänster, Tjänstekatalog 1.0*. Enligt avtalet omfattas VGRnet av det s.k. kärnnätet samt de tjänster och funktioner som finns fram till överlämningspunkt till lokalt nät.

Basnivån vad beträffar tillgänglighetskrav och åtgärdstider för VGRnet är 99,6% med maximalt 8 timmars åtgärdstid vardagar under kontorstid. Beredskap skall ”finnas tillgängligt under ej kontorstid med en timmes inställelsetid”. Utöver basnivån finns ytterligare tre nivåer. Den högsta servicenivån har kärnnätet, d.v.s. mellan huvudnoderna, där tillgängligheten skall vara minst 99,9% med en åtgärdstid som ej överstiger två timmar.

VGR IT avropar externa transmissionstjänster på ramavtal från Telia. Det gällande avtalet innehåller krav på tillgänglighet (99,6%). Leverantören skall betala viten om tillgänglighetskrav ej uppfylls. I avtalet finns krav på att leverantören skall ha en informationssäkerhetspolicy samt att VGR har rätt till revision. VGR IT och Telia har rapporteringsmöten en gång i kvartalet då servicenivåer och planerade aktiviteter diskuteras.

Eftersom förvaltningarna inte har egna IT-avdelningar längre ansvarar VGR IT utöver VGRnet för de lokala nätverken (LAN) och tjänster t.ex. övervakning, som är förknippade med dessa. Avtal för drift av dessa lokala nätverk finns i varierande grad mellan förvaltningar och VGR IT. Dessa innehåller inga krav kring kapacitet och det görs ingen uppföljning av servicenivåer. Det saknas gemensam mall för dessa avtal.

Det pågår ett arbete av representanter från beställaren och VGR IT med att ta fram en mer detaljerad tjänstekatalog. Målet är att IT-tjänsterna skall vara mer definierade och prissatta samt anpassade till regionens mål om kostnadskontroll. Den föreslagna tjänstekatalogen är efterfrågad av förvaltningarna, men den har ännu inte kommunicerats till dem.

Väsentliga brister:

- Innehållet i och omfattningen av avtal för lokala nätverk mellan VGR IT och förvaltningarna varierar. Förvaltningarna efterfrågar särskilt servicenivå-avtal för att veta vad de kan förvänta sig av VGR IT.
- Det finns ännu inte någon prissatt tjänstekatalog över de nätverkstjänster VGR IT tillhandahåller.

2.6 Investeringar och kostnader

2.6.1 Investeringar

Investeringar i VGRnet kan ske med medel från två olika investeringsramar. Beslutsvägarna upplevs som otydliga och inkonsekventa.

Den ena ramen utgörs av en årlig investeringsbudget på drygt 10 mkr öronmärkt för VGRnet. Låneramen har funnits under ett antal år efter ett beslut taget i Regionstyrelsen. Styrning över denna låneram har överförts från ITSA till VGR IT. Det är främst inköpscontrollern på VGR IT som har uppgiften att sammanställa och föreslå prioriteringar avseende re- och nyinvesteringar. Behov och önskemål framförs dels från förvaltningarna via VGR IT:s kundansvariga, dels är det behov som lyfts fram internt inom VGR IT, från enhetscheferna. Det fortsatta arbetssättet med prioritering av investeringsbehoven är att de samlade beslutsunderlagen diskuteras både med förvaltningarna och förankras med FoA Infrastruktur innan ett investeringsförslag och avrop slutligen lämnas till Regionservice gemensamma beredningsgrupp för beslut. I denna beredningsgrupp konkurrerar investeringar i infrastruktur med alla andra investeringar som görs av Regionservice. Hittills har inte någon föreslagen investering i VGRnet prutats bort, utan snarare har åtgärder senarelagts på grund av bristande personresurser.

Den andra investeringsbudgeten utgörs av IT-rådets utvecklingsbudget på 15 mkr. Dessa investeringar avser främst nyinvesteringar kopplade till regionens årliga strategiska ”Handlingsplan för verksamhetsutveckling med stöd av IT”.

Två investeringsramar gör att beslutsvägarna för investeringar är otydliga, det är uppenbart att förvaltningsföreträdare har olika uppfattningar om hur deras behov skall omhändertas och de upplever att investeringsprocessen genomförs inkonsekvent, tar lång tid och är ineffektiv. Det inträffar även att beslutsfattare på regional nivå i det ena ärendet vänder sig till IT-direktören eller IT-rådet för att i nästa ärende vända sig till ledningen för Regionservice. På liknande sätt finns det inget formellt hinder för VGR IT att gå direkt till regiondirektören, utan att bereda investeringsbeslutet med FoA Infrastruktur. Enligt vissa förvaltningar har detta skett, exempelvis i samband med satsningen på IP-telefoni.

För varje investering skall en investeringsbudget tas fram. Det framhålls att det är oklara krav på hemtagande i investeringsbudgetar samt att de kostnads-/nyttoanalyser som genomförs är av undermålig kvalitet.

En risk som framhålls beträffande investeringar är att förvaltningarnas pressade ekonomi medför att utrymmet är otillräckligt för att investera i de lokala nätverken. Dessa kan således komma att utgöra en flaskhals med risk för att säkerheten inte kan hållas på en tillfredsställande nivå ända fram till arbetsstationer och medicinteknisk utrustning.

2.6.2 Kostnadsuppföljning

Redovisningen av de tjänster VGR IT levererar till förvaltningarna har hittills inte varit specificerad. Förvaltningarna debiteras månadsvis med 1/12 av det belopp som motsvarar den IT-kostnad som de redovisat att de haft tidigare, d.v.s. innan VGR IT bildades. Beställarsidan och de förvaltningar som vidtalats under granskningen upplever att redovisning av kostnader är mycket begränsad i dagsläget. Det går inte att utläsa vad support kostar, vad VGRnet kostar o.s.v.

En controller på VGR IT följer upp de totala kostnaderna och stämmer av mot vad som debiteras ut internt. Alla kostnader utom mantid sätts på ett konto och uppföljning görs på månadsbasis.

VGR IT:s målsättning är att, förutom på mantid, redan under kvartal 1-2 under 2009 göra en mer detaljerad uppföljning för produkter och tjänster inom Infrastrukturområdet och sedan 2009-01-01 har s.k. produktkategorier förts in i ekonomisystemet.

Under februari skall ledningsgruppen för Infrastruktur ta fram de ekonomiska komponenterna och kostnadsstrukturer för produkter och tjänster. VGRnet är en av de tjänster som kommer att följas upp ekonomiskt och via servicenivåer. Allt skall vara klart till sommaren 2009 innan budgetarbetet för 2010 påbörjas.

Väsentliga brister:

- **Handläggningen och beslutsprocessen för investeringar upplevs som otydlig och genomförs inkonsekvent och är ineffektiv.**
- **Det råder avsaknad av kriterier för prioritering mellan investeringar. Detta leder till oklarheter vilka principer som tillämpas vid VGR IT:s prioritering mellan egna projekt och kunders projekt.**
- **I nuvarande organisation kan VGR IT starta projekt, som påverkar förvaltningarna, med mandat från regiondirektören utan att gå via IT-rådet.**
- **Det är otydligt vilka krav som ställs på lönsamhetskalkyler i investeringsbudgetar.**
- **Hittills har endast en begränsad uppföljning av kostnader skett, kopplat till förvaltning och utveckling av VGRnet.**

2.7 Säkerhet och riskhantering

2.7.1 Säkerhetspolicy

Regionstyrelsen har det övergripande ansvaret att leda, samordna och utveckla arbetet med informationssäkerhet samt tillse att denna utvecklas utifrån regionens behov. Regionstyrelsen ska förvissa sig om att det såväl inom styrelsens eget ansvarsområde som inom respektive nämnders bedrivs ett informationssäkerhetsarbete i enlighet med de regler/riktlinjer som fullmäktige eller styrelsen utfärdat. Säkerhetsarbetet inom VGR leds av säkerhetsdirektören.

Följande dokument styr säkerhetsarbetet:

- En **säkerhetspolicy** (uppdaterad 2008), som beskriver organisationens säkerhetsmål, ansvar, samt genomförande och uppföljning av säkerhetsarbete. I policyn framgår det att regionala riskhanteringsråd skall finnas samt att riskanalyser skall göras regelbundet.
- Ett **ramverk för säkerhetsarbete** som innehåller ansvar, roller och arbetssätt.
- En **regional strategi för säkerhetsarbetet i VGR 2008-2011**, utformad som ett balanserat styrkort.

VGR har ett antal **anvisningar** som styr säkerhetskrav på en mer detaljerad nivå. Anvisningen har sitt ursprung i den internationella informationssäkerhetsstandarden ISO/IEC 27000, där i första hand *Anvisning nummer 3, Kommunikation och drift av IT-system*, kapitel 10, rör krav med påverkan på VGRnet. I detta kapitel står det att:

”Systemägaren ansvarar för att det finns tydliga regler för drift och underhåll av nätverket. I detta ansvar ligger bland annat att ta fram regler för anslutning av utrustning till nätverket och till nätverket hörande kringutrustning.

För att åstadkomma säkerhet för data i nätverk och för att skydda anslutna tjänster bör systemägaren särskilt beakta att följande kontroller implementeras:

- Driftansvar för nätverk bör, när så är möjligt, vara skilt från ansvar för datordriften;
- Ansvar och rutiner bör fastställas för hantering av icke centralt placerad utrustning, inklusive utrustning installerad hos VGR’s (interna och externa) användare;
- Om nödvändigt bör särskilda åtgärder vidtas för att skydda sekretess och riktighet när data passerar allmänna nät liksom även för att skydda anslutna system. Särskilda åtgärder kan också krävas för att upprätthålla åtkomlighet till av VGR prioriterade nätverk och anslutna datorer.”

Enligt uppgift från VGR IT har det ställts kvar på leverantörer att de skall ha en informationssäkerhetspolicy, samt att VGR IT har rätt att revidera dem.

2.7.2 Riskhantering

Enligt VGR:s säkerhetspolicy ansvarar regionstyrelsen för att god säkerhet upprätthålls inom regionen, medan nämnd, styrelse och bolag ansvarar för säkerheten inom respektive verksamhet, inklusive att fastställa en plan för säkerhetsarbete, genomföra risk- och sårbarhetsanalyser samt rapportera resultatet av säkerhetsarbete till regionstyrelsen.

I säkerhetspolicyn framgår att:

”*[…] regionen och dess verksamheter ska kontinuerligt analysera risker och sårbarheter i verksamheten på lämpligt sätt. Slutsatserna av genomförda analyser skall leda till lämpliga skyddsåtgärder.*”

VGR använder sig av två metoder som stöd i arbetet med att genomföra riskanalyser. Dessa är **PRA** (processinriktad riskanalys) samt **MVA** (mångdimensionell verksamhetsanalys).

I dagsläget genomförs riskanalyser i varierande form och storlek i VGR:s förvaltningar. VGR IT blir ibland inbjudna och deltar i en del riskanalyser ute i förvaltningarna. Det finns ingen sammanhållen dokumentation av de IT-relaterade riskbedömningar gällande kritiska system som förvaltningarna genomfört. VGR IT upplever att detta kan göra det svårt att prioritera mellan skyddsåtgärder för de system och tjänster som använder sig av VGRnet.

De senaste riskanalyserna av VGRnet genomfördes 2008 samt 2004. Enligt VGR IT görs riskanalyser när nya tekniska system skall införas. Det har förekommit att verksamheterna har infört nya system som kan ha inverkan på VGRnet:s kapacitet utan att ha kommunicerat detta till VGR IT.

Enligt säkerhetsdirektören har ett 100-tal riskanalyser genomförts inom VGR de senaste åren. Då dessa utgår från verksamhetsprocesser ingår VGRnet i flertalet av analyserna, då infrastrukturen är en viktig, stödjande del till verksamheten.

Sedan incidenterna med datorhallarna inträffade under våren 2008, med längre avbrott i kommunikationen som följd, har VGR IT, på uppmaning av regiondirektören och med medel ur regional handlingsplan 2008, initierat ett projekt som syftar till en ”säkerhetsöversyn av datorhallar” och driftpunkter. En pilotinsats genomfördes i augusti-september på SÄS och SU. Efter utvärdering av piloten har ett beslut tagits i IT-rådet att gå vidare med en säkerhetsöversyn av VGR:s datorhallar och växelrum, med start i november 2008. Översynen skall vara genomförd t.o.m. februari 2009.

2.7.3 Kontinuitetsplanering

Ett krav som ställs i VGRs säkerhetspolicy är att säkerhetsprocessen i regionen ska omfatta förebyggande, avhjälpande och återuppbyggande faser. Vidare finns krav på att avbrottsplaner tas fram samt att dessa skall uppdateras kontinuerligt och övas.

Dokumentet *Regional anvisning för kontinuitetsplanering* innehåller krav på hur förvaltningarna skall bedriva sin kontinuitetsplanering. Anvisningen bygger på ISO/IEC 27000 och beskriver process för kontinuitetsplanering, avbrottsanalys, testning, underhåll och utbildning.

I dagsläget ser arbetet med kontinuitetsplanering dock olika ut på de olika förvaltningarna. NU-sjukvården har exempelvis instruktioner och riktlinjer för varje klinik för hur de skall hantera ett avbrott i verksamheten.

Primärvården har under 2008 tagit fram avbrottsplaner och ett antal processer kring det, arbetet är dock ej avslutat.

Tandvården har manuella rutiner för avbrott.

2.7.4 Incidenthantering

VGR har upprättat en regional IT-incidentanvisning som är utformad med stöd av ramverket för informationssäkerhet. Anvisningen har uppdateras efter omorganisationen och enligt VGR IT pågår nu ett jobb med att migrera över denna anvisning till ITIL-processen Incident management.

En uppfattning är att de nya eskaleringsvägarna inte fungerar om och när en incident inträffar. Det finns heller inga rutiner för VGR IT att rapportera incidenter till FoA Infrastruktur. Informellt har dessa rapporter gått till Regiondirektören, vilket snarare är en följd av tidigare rapporteringsvägar, då IT-direktören var systemägare.

Enligt säkerhetspolicyn skall förvaltningar varje år redovisa sitt säkerhetsarbete i sin årsredovisning. Enligt flera respondenter görs ingen aktiv uppföljning av att riskanalyser och kontinuitetsplanering har genomförts.

Väsentliga brister:

- Riskhantering och kontinuitetsplanering åligger förvaltningarna inom VGR. Dock sker endast begränsad uppföljning av riskanalyser och kontinuitetsplanering.
- Fullständiga kontinuitetsplaner finns ej för samtliga förvaltningar.
- Rapporterings- och eskaleringsvägar i samband med IT-incidenter fungerar inte sedan omorganisationen med VGR IT genomfördes.

2.8 Projekthantering

Regionen har ett hjälpmedel för projektstyrning för projektledare, som enligt beslut av regiondirektören skall användas för alla regionövergripande projekt. Hjälpmedlen som i huvudsak består av dokumentmallar går under benämningen Projektilen.

Däremot är Projektilen ingen projektstyrningsmodell, d.v.s. en modell som ger strukturer för viktiga milstolpar och beslutspunkter i utvecklingsprojekt.

En process kommer att föreslås för IT rådet under första kvartalet 2009 om hur utvecklingsprojekt i regional Handlingsplan skall hanteras. Denna process kommer att ha grindar/gates för viktiga beslutspunkter inför fortsatt utveckling och ev driftsättning

Väsentliga brister:

- Projektilen är inte en projektstyrningsmodell utan en uppsättning hjälpmedel för projektledare. Mallarna som finns i Projektilen kan upplevas vara för omfattande för mindre projekt.
- Begränsad utbildning ges.

3 Slutsatser och rekommendationer

3.1 Generella slutsatser

Trots en del kritik, främst kring styrningen av VGRnet, framgår det tydligt av intervjuerna att uppfattningen hos både ITSA, förvaltningar och VGR IT, är att VGRnet är ett nät med bra prestanda, hög stabilitet och hög säkerhet. Antalet incidenter har också varit få under de senaste fem åren.

I samband med att VGR omorganiserat sin IT-verksamhet har styrningen av VGRnet påverkats. En del förvaltningar upplever att den nya organisationen fungerar på pappret men att den inte förankrats i verksamheten tillräckligt. Vissa intressenter uttrycker också missnöje med långa beslutsvägar och brist på kostnadsuppföljning. Det framkommer även att de strategiska handlingsplaner som finns för utveckling av VGRnet under hösten 2008 inte är kända hos personer som förväntas vara informerade.

3.2 Rekommendationer

Nedan följer våra rekommendationer samt ett förslag på prioritering.

Rekommendationerna är prioriterade enligt följande:

Hög	Bristen bör åtgärdas snarast för att säkerställa effektivitet och/eller intern kontroll på kort sikt.
Medel	Bristen bör åtgärdas snarast för att säkerställa effektivitet och/eller intern kontroll på lång sikt.
Låg	Effektivitet kan förbättras. Bristen bör åtgärdas på lång sikt.

#	Iakttagelse och rekommendation	Prioritet
1.	Iakttagelse: Beslutsvägarna för investeringar uppfattas som otydliga. Investeringsprocessen upplevs som inkonsekvent och ineffektiv. Nuvarande investeringsmodell gör också att VGR IT kan gå direkt till regiondirektören med en investering utan att behandla ärendet tillsammans med ITSA och förvaltningar i RegSam och IT-rådet. Rekommendation: Vi rekommenderar en översyn av investeringsprocessen för infrastruktur, i syfte att göra den mer ändamålsenlig för både nyttjare, beställare och utförare.	Hög
2.	Iakttagelse: Det råder en otydlighet kring den nya organisationen som utformats genom projektet BestIT. Det som är beskrivet i dokument är inte realiserat i praktiken. Det gäller otydligheter om vilka funktioner som ansvarar för vad, vilka beslut och vilka mandat som gäller o.s.v. För flertalet av respondenterna är det t.ex. oklart vem som är systemägare av VGRnet. Sannolikt bottnar denna otydlighet i att den nya organisationen inte satt sig ännu och att den delvis är bristfälligt kommunicerad. Rekommendation: Ytterligare aktiviteter behöver genomföras för att kommunicera den nya organisationen, dess funktioner och de ansvarsområden som förekommer. Bl.a. bör det klargöras vem som är systemägare för VGRnet.	Hög

3.	Iakttagelse: För varje investering skall en investeringsbudget tas fram. Det framhålls att det är oklara krav på hemtagande i investeringsbudgetar samt att de kostnads-/nyttoanalyser som genomförs är av undermålig kvalitet. Rekommendation: I syfte att minska risken att investeringar som ej är tillräckligt motiverade för verksamheten görs, rekommenderar vi att krav tas fram på hur kostnads-/nyttoanalyser skall genomföras vid nya investeringar, samt en för ändamålet lämplig modell för kostnads-/nyttokalkylering vid investering. Vi rekommenderar också att det görs uppföljningar mot dessa kalkyler när investeringen är genomförd.	Medel
4.	Iakttagelse: I regionens nuvarande modell för beställning av IT-tjänster finns det inget renodlat forum för beställarna, eftersom VGR IT deltar både i FoA Infrastruktur, RegSam och IT-rådet. Det innebär att beställar-/utförarmodellen inte är fullt implementerad. Modellens berednings- och beslutsvägar uppfattas som ineffektiva av företrädarna för förvaltningarna. Uppfattningen är att tankarna från BestIT inte har realiserats i praktiken. Rekommendation: En mer genomgående utvärdering av nuläget och resultat bör ske i jämförelse med den beställar-/utförarmodell som beslutades, baserad på BestIT. En tydligare uppdelning mellan beställare och utförare bör därigenom övervägas. Detta förutsätter dock att beställarna förfogar över tillräcklig beställarkompetens, inklusive teknisk kompetens.	Medel
5.	Iakttagelse: Det finns ännu inte någon prissatt tjänstekatalog framtagen över de nätverkstjänster som VGR IT tillhandahåller. Det finns heller inte några servicenivåavtal framtagna för de lokala nätverken som VGR IT. Båda dessa är efterfrågade av förvaltningarna för att de skall veta vad de kan förvänta sig av VGR IT. Rekommendation: Vi rekommenderar VGR IT att fortsätta sitt arbete med att ta fram en mer detaljerad tjänstekatalog rörande VGRnet som förvaltningarna kan göra avrop mot. Exempel på tjänster kan vara tillgång till VGRnet, tillgång till lokalt nät, beställarkoordinator och service desk. I syfte att säkerställa ansvar och servicenivåer för de lokala nätverken rekommenderar vi VGR IT att ta fram en gemensam mall, samt teckna avtal med samtliga förvaltningar som ej driftar sitt eget nätverk.	Medel

6.	Iakttagelse: Bristande kontinuitetsplanering hos förvaltningar var en brist som identifierades i incidentrapporten efter de två incidenter som påverkade VGRnet i april 2008. Fullständiga kontinuitetsplaner finns ej för samtliga förvaltningar. Avsaknad av kontinuitetsplanering kan leda till att incidenter ej hanteras på ett effektivt sätt för verksamheten. Det sker endast begränsad uppföljning av riskanalyser och kontinuitetsplanering. Rekommendation: I syfte att säkerställa att kontinuitetsplaner finns på plats samt att de är aktuella och testade, rekommenderar vi ansvariga nämnder och Säkerhetsdirektören att aktivt följa upp förvaltningarnas arbete med kontinuitetsplanering. Vi rekommenderar alla förvaltningar i VGR att skapa rutiner för kontinuitetsplanering. Rutinerna bör utgå från en processbaserad riskanalys och adressera: • Reservrutiner vid avbrott för tänkta scenarios. • Rutiner för återställning av system. • Rutiner för återskapande av förlorad information. • Rutiner för inmatning av data från reservrutiner. • Periodisk testning av rutiner. Vi rekommenderar också att uppföljning görs av genomförda riskanalyser.	Medel
7.	Iakttagelse: Rapporterings- och eskaleringsvägar i samband med IT-incidenter fungerar inte sedan omorganisationen med VGR IT genomfördes. Rekommendation: En särskild utvärdering bör ske av anvisningen för incidenthantering inklusive rutiner för eskalering och rapportering.	Medel
8.	Iakttagelse: I avtalet mellan ITSA och VGR IT är tillgängligheten till kärnnätet reglerat till minst 99,81%. Ingen formell uppföljning görs av faktisk tillgänglighet. Rekommendation: Vi rekommenderar VGR IT att mäta och rapportera de servicenivåer som finns avtalade mellan VGR IT och ITSA, i syfte att säkerställa att förvaltningarna får den kapacitet de betalat för.	Medel
9.	Iakttagelse: VGR IT har hittills endast en begränsad uppföljning av kostnader för förvaltning och utveckling av VGRnet. Det finns i nuläget ingen redovisning vad olika IT-tjänster kostar. Rekommendation: Vi rekommenderar VGR IT att prioritera planerna på att införa en mer detaljerad kostnadsuppföljning, i syfte att kunna införa en tjänsteprislista som bättre speglar faktiska kostnader. En mer detaljerad kostnadsuppföljning är också en förutsättning för att kunna mäta effektivitet av förändringar i verksamheten.	Låg

10.	Iakttagelse: Det finns en formell kommunikationsstrategi, den har dock ej blivit uppdaterad sedan 2004. Rekommendation: Vi rekommenderar VGR IT att uppdatera kommunikationsstrategin för VGRnet. Detta i syfte att reflektera förändringar i verksamhetsmässiga och regulatoriska krav som inträffat sedan 2004.	Låg
11.	Iakttagelse: Sporadiska initiativ har tagits för att identifiera nyckelpersoner samt ta fram strategier för att minimera beroendet. Rekommendation: I syfte att minimera nyckelpersonberoende rekommenderar vi VGR IT att på ett strukturerat sätt identifiera nyckelkompetens, vilka personer som har denna samt hur beroenden skall hanteras.	Låg
12.	Iakttagelse: VGR IT:s resurser upplevs av vissa förvaltningar vara överbelastade med mindre frågor, och har svårt att hinna med strategiska frågor. Rekommendation: Vi rekommenderar VGR IT att tillsammans med förvaltningarna undersöka bakgrunden och validiteten i påståendet, exempelvis i de samarbetsforum som finns i dagsläget.	Låg
13,	Iakttagelse: Det finns ett utkast till IT-infrastrukturplan. Rekommendation: Vi rekommenderar VGR IT att färdigställa IT-infrastrukturplanen, i syfte att säkerställa effektivitet och konformitet i investeringar och utveckling av infrastrukturen.	Låg

Bilaga Granskningsprogram ur COBIT

Analys av styrning av VGRnet samt riskhantering är gjord mot god praxis (ramverket CobiT).

IT-organisation och IT-verksamhet

CobiT	Revisionspunkt
PO4.1	VGR har ett ramverk för IT-processer (som påverkar infrastrukturen).
PO4.2	VGR har en enhet som ansvarar för IT-strategin. Strategi för infrastruktur ligger inom denna enhets ansvar.
PO4.3	VGR har en styrgrupp för IT som prioriterar mellan investeringar, övervakar status av projekt samt övervakar servicenivåer.
PO4.4	IT-direktör rapporterar till ledningen.
PO4.5	VGR:s IT-organisation är väl dokumenterad och motsvarar verksamhetens behov.
PO4.5	Det finns en process för att årligen se över IT-organisationen så att den motsvarar verksamhetens behov (behov av sourcing).
PO4.6	VGR har, för IT-organisationen, etablerade roller med ansvars- och rollbeskrivningar.
PO4.7	VGR har en funktion för kvalitetssäkring av IT-verksamheten.
PO4.8	VGR har utsedda personer som ansvarar för informationssäkerhet och IT-säkerhet.
PO4.9	Data- och systemägare finns definierade för system och för VGRnet.
PO4.10	Det finns en process för uppföljning av att roller och ansvar utförs enligt fastställda beskrivningar.
PO4.12	Det finns rutiner för att regelbundet se över bemanningskrav.
PO4.13	Det finns rutiner för att definiera och identifiera nyckelpersoner samt rutiner för att minimera beroendet.
PO4.14	Kontrakterad personal lever upp till VGR:s styrande dokument.
PO4.15	Det finns en strategi för att hantera relationer mellan IT-verksamheten och dess intressenter.

IT-strategi

CobiT	Revisionspunkt
PO1.2	Säkerställande att strategi för VGRnet och verksamhetsstrategier går hand i hand.
PO1.3	VGR har fastställt nuvarande kapacitet i VGRnet, i syfte att kunna planera för investeringar och mäta förändringar.
PO1.4	Det finns en formell strategi för VGR:s infrastruktur.

Investeringar

CobiT	Revisionspunkt
PO5.1	VGR har en investeringsportfolio eller liknande för investeringar relaterade till VGRnet.
PO5.2	VGR gör prioriteringar mellan investeringar relaterade till VGRnet.
PO5.3	VGR har ett regelverk för budgetering av VGRnet:s verksamhet.
PO5.4	VGR har rutiner för att följa upp VGRnet:s kostnader mot investerings budget

CobiT	Revisionspunkt
PO5.5	VGR har rutiner för att följa upp nyttan av större investeringar i VGRnet.

Teknisk inriktning

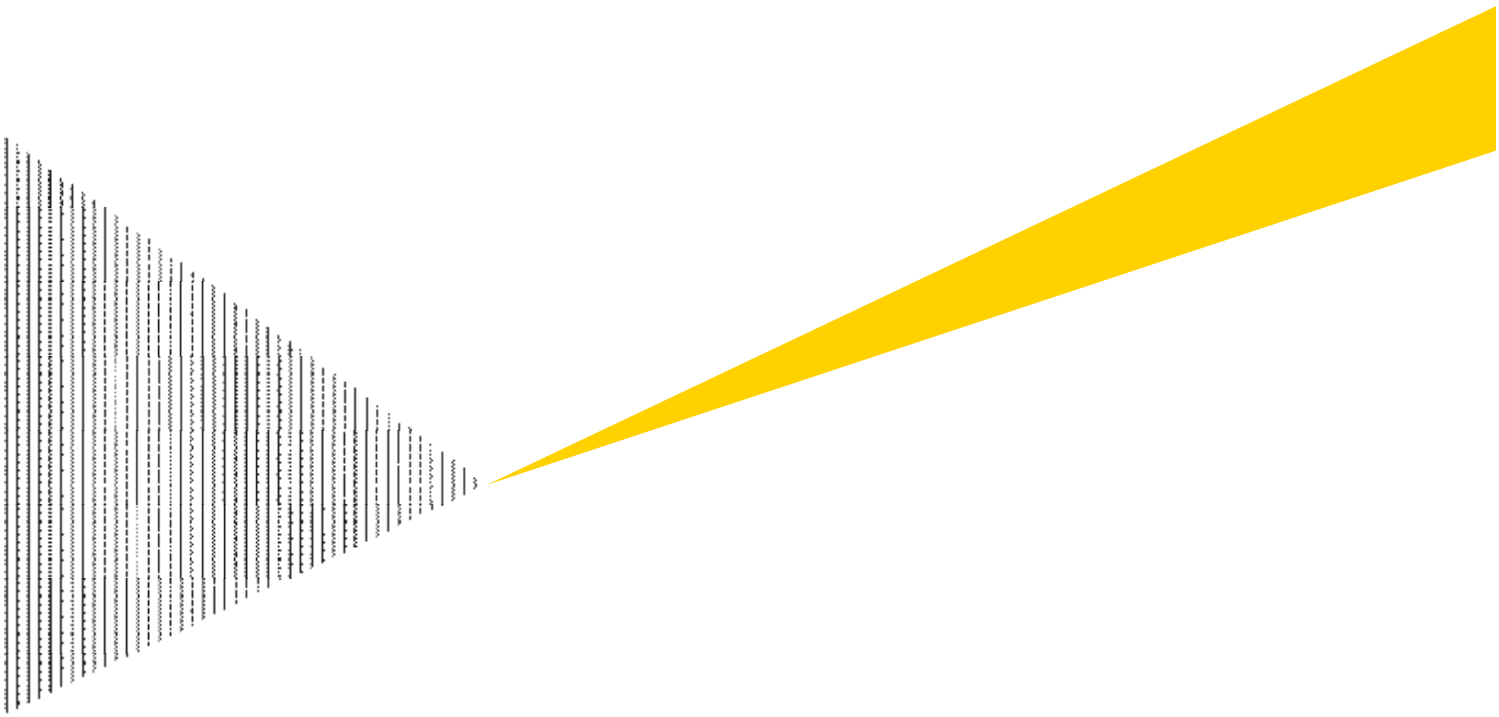
CobiT	Revisionspunkt
PO3.2	Det finns en infrastrukturplan som fastställer VGR:s plan för infrastruktur.
PO3.3	VGR har en etablerad process för att bevaka teknisk utveckling av infrastruktur.
PO3.3	VGR har en etablerad process för att bevaka lagstiftning som kan få inverkan på infr
PO3.4	VGR har ett forum som analyserar och väljer mellan teknik, plattformar och arkitektu

Riskhantering

CobiT	Revisionspunkt
PO4.8	VGR utsedda roller som ansvarar för IT-risker.
PO9.1	VGR har ett ramverk för hantering av IT-risker.
PO9.2	VGR har definierat när ramverket skall användas (nya projekt/hela verksamheten).
PO9.3	VGR har identifierar hot och sårbarheter i VGRnet.
PO9.4	VGR har identifierat konsekvenser om risker relaterade till VGRnet realiseras. VGR har analyserat sannolikheten av att risker relaterade till VGRnet realiseras.
PO9.5	VGR har dokumenterat hur identifierade risker skall tas om hand av verksamheten.

Projekthantering

CobiT	Revisionspunkt
PO10.1	VGR har rutiner för att hantera projekt relaterade till investeringar i VGRnet. Rutinerna inkluderar utvärdering, prioritering och övervakning.
PO10.2	VGR har en etablerad projektmetodik som används i projekt relaterade till VGRnet.
PO10.3	VGR har en etablerad rutin för att tillsätta projektorganisation, inklusive definierade roller och ansvar.
PO10.4	VGR säkerställer att intressenter medverkar i planering och utförande i projekt relaterade till VGRnet.
PO10.5	Definition av omfattning och avgränsningar av projekt relaterade till VGRnet.
PO10.6	VGR använder sig av milstolpar i projekt relaterade till VGRnet.
PO10.7	VGR har formella projektplaner för projekt relaterade till VGRnet.
PO10.9	VGR genomför riskanalyser i sina projekt relaterade till VGRnet.
PO10.10	VGR har kvalitetsplaner till sina projekt relaterade till VGRnet.
PO10.11	VGR har rutiner för att hantera förändringar i projekt relaterade till VGRnet.
PO10.14	VGR har rutiner för godkännande av projekt relaterade till VGRnet.



Marcus Hansson
marcus.hansson@se.ey.com
031-63 63 26

Neda Heidar Khan
neda.heidar.khan@se.ey.com
031-63 63 92

Johan Elmberg
johan.elmberg@se.ey.com
031-63 63 93

ERNST & YOUNG