



2026-02-02

# **Riskhantering i samband med Millenniuminförandet**

Fördjupad genomlysning

Datum: 2026-02-02

Dokumentnamn: Riskhantering i samband med Millennium-införandet. Fördjupad genomlysning

Diarienummer: RS 2026-00717

# Innehållsförteckning

Riskhantering i samband med Millenniuminförandet.....	0
Innehållsförteckning.....	2
Sammanfattning .....	4
1. Bakgrund.....	5
2. Syfte och mål .....	6
3. Avgränsning och förtydliganden .....	6
4. Riskhantering i genomlysningen .....	9
4.1 Vad som avses med riskhantering .....	9
4.2 Varför ett övergripande riskperspektiv är viktigt .....	10
4.3 Enterprise Risk Management (ERM).....	10
4.4 Riskhantering i denna genomlysning .....	11
5. Resultat per riskkategori.....	11
5.1 Avsaknad av samlad helhetsbild .....	12
5.2 Bristande riskeskalering och transparens .....	13
5.3 Tystnadskultur och undvikande av obekväma risker.....	15
5.4 Oklart riskägarskap och ansvar för konsekvenser .....	18
5.5 Svag koppling mellan risk och beslut .....	19
5.6 Fragmenterad riskhantering mellan nivåer och projekt .....	22
5.7 Strukturella hinder i riskprocessen.....	24
5.8 Otillräcklig objektivitet i riskhanteringen .....	26
5.9 Normalisering av kända risker .....	27
5.10 Bristande integration av Program Millenniums riskprocess med övriga VGR .....	29

6. Reflektioner: Iakttagelser kring organisatoriska mönster .....	31
6.1 Strategiskt gap mellan program och organisation .....	32
6.2 Iakttagelser kring ledning och beslutskultur .....	32
7. Förbättringsförslag .....	33
7.1 Strategisk integrering av riskhantering .....	33
7.2 Stärkt ledarskap och kulturellt skifte .....	34
7.3 Processens Robusthet och Transparens.....	34

# Sammanfattning

Den 12 november 2024 driftsattes vårdinformationssystemet Millennium i Västra Götalandsregionens (VGR:s) södra område. Omgående uppstod dock svårigheter som påverkade driftsättningen och den 15 november 2024 avbröts införandet, med hänvisning till att patientsäkerheten inte kunde garanteras. Därefter har det i olika sammanhang framkommit att risker som identifierats och lyfts inför driftstarten inte hanterats som de borde. Detta har tydliggjort behovet av att förstå hur riskhantering fungerat i praktiken, främst inom program Millennium.

Genomlysningen är inte framtagen för ansvarsutkrävande, och den syftar inte till att förklara varför införandet av Millennium fick det utfall det fick. Syftet med denna genomlysning är att identifiera och beskriva brister och problem kopplade till riskhantering i samband med Millennium-införandet.

Följaktligen har det i genomlysningen varken bedömts vilken part som ska anses ansvarig enligt avtalet avseende Millennium eller i övrigt gjorts en juridisk bedömning av sådana frågor. Innehållet i denna genomlysning ska därför inte ses som en juridisk bedömning av vilken part som bär ansvaret, och inga uttalanden eller slutsatser ska tillmätas rättslig betydelse.

I denna genomlysning omfattar riskhantering både programmets formella processer och den faktiska praktiken i styrning och ledning. Begreppet inkluderar därför:

- hur risker identifierades och värderades,
- vilka möjligheter till samlad riskbild som funnits,
- hur risker kommunicerades och eskalerades,
- vilka formella och informella vägar som användes,
- hur ansvar för risker togs i program, införandeprojekt och linjeorganisation.

Genomlysningen och analysen har, baserat på tillgängligt material och intervjuer, resulterat i ett antal reflektioner och iakttagelser gällande mönster och brister i riskhanteringen i samband med Millennium-införandet. Gjorda iakttagelser pekar på områden där VGR kan behöva stärka sina strukturer, arbetssätt och sin kultur inom området riskhantering. Det är viktigt att notera att denna analys inte är heltäckande, utan är framtagen för att bidra till lärande och förbättring i regionens fortsatta strategiska arbete med riskhantering.

# 1. Bakgrund

Västra Götalandsregionen (VGR) beslutade redan 2013 att påbörja ett arbete med en ny och gemensam vårdinformationsmiljö för hälso- och sjukvården, en av regionens mest omfattande digitala förändringar. Ett samlat kärnsystem var tänkt att utgöra navet och den 12 november 2024 driftsattes vårdinformationssystemet Millennium i regionens södra område. Omgående uppstod dock svårigheter som påverkade driftsättningen och den 15 november 2024 avbröts införandet, med hänvisning till att patientsäkerheten inte kunde garanteras. Därefter har det i olika sammanhang framkommit att risker som identifierats och lyfts inför driftstarten inte hanterats som de borde.

Insamlingen av medarbetarnas erfarenheter, som gjorts inom ramen för uppdraget till samordningsgruppen för vårdinformationsmiljö, visar på upplevelser av att få dåligt gehör för oro som uttrycktes inför driftstart, både från programorganisation och i egen linjeorganisation. Medarbetare upplevde att de innan driftstart påtalade brister i bland annat teknisk funktionalitet, användarvänlighet, patientsäkerhet och utbildning utan att bli lyssnade på. I dialogmöten med fackliga företrädare har det framkommit liknande upplevelser och erfarenheter, främst utifrån ett arbetsmiljöperspektiv, vilka framförts till samordningsgruppens beslutsfattare.

Den granskning som KPMG genomförde av Millennium-införandet visar på liknande erfarenheter, att risker identifierades men att hanteringen inte fungerade som avsett. Brister kopplade till transparens, eskalering, ansvar, kultur och kopplingen mellan risk och beslut har återkommit i flera delar av materialet. Rapporten visar bland annat på att arbetet fortsatte i enlighet med tidplanen trots varningssignaler och rapporten talar om en tystnadskultur som kan ha påverkat hur risker hanterats och medarbetare bemötts. KPMG beskriver också att information till ägarutskottet inte var helt samstämmig med den faktiska utvecklingen, där risker och problem beskrevs som hanterbara inför driftstart.

Detta har tydliggjort behovet av att förstå hur riskhantering fungerat i praktiken, främst inom program Millennium. Sammantaget gjorde detta att beslutsfattarna i Samordningsgrupp för vårdinformationsmiljö gav VGR:s informationssäkerhetschef i uppdrag att göra en fördjupad genomlysning av frågan.

Riskhantering handlar om att identifiera, analysera och hantera potentiella risker som kan påverka projektets framgång, säkerhet och verksamhetens

kontinuitet. Riskhantering sker oftast utifrån ett fördefinierat perspektiv till exempel arbetsmiljö, patientsäkerhet, teknik eller informationssäkerhet.

I denna genomlysning tas ett bredare perspektiv kring begreppet riskhantering genom att se på de strukturer, arbetssätt och beteenden som ska säkerställa att risker identifieras, värderas, kommuniceras och hanteras på ett sätt som skyddar verksamhet, patienter och organisationens mål.

## 2. Syfte och mål

Syftet med denna genomlysning är att identifiera och beskriva de brister och problem som kunnat kopplas till riskhantering i arbetet med Millennium-införandet. Genomlysningen utgår från tio områden där brister framkommit i olika sammanhang. Utifrån intervjuer och insamlat material belyses och analyseras hur risker har identifierats, hanterats, kommunicerats och etablerats genom programmet struktur, införandeprojektens styrkedjor och i organisationens ledningsvägar.

Målet är att ta tillvara lärdomar från införandet och ge ett underlag för VGR:s fortsatta arbete med att stärka regionens strategiska riskhantering och för att utveckla en mer sammanhållen övergripande riskhanteringsmodell genom ett uppdrag som är under framtagande.

Därutöver ska genomlysningen även stödja pågående uppdrag såsom:

- Hälso- och sjukvårdens organisering av verksamhetsutveckling med stöd av digitalisering, och
- Planering och förändringsledning vid införande av nytt vårdinformationssystem.

Genomlysningen ska bidra till lärande, förbättringar och utveckling av VGR:s samlade förmåga att hantera risker i komplexa förändrings- och verksamhetsutvecklingsarbeten.

## 3. Avgränsning och förtydliganden

Det bör observeras att genomlysningen inte syftar till ansvarsutkrävande. Syftet är inte heller att förklara varför införandet av Millennium fick det utfall det fick. Fokus ligger på att identifiera brister och problem kopplat

till riskhantering, så att VGR kan stärka sitt fortsatta strategiska arbete kring risker.

Uppdraget innefattar inte heller att analysera hela riskhanteringen i och runt införandet av Millennium. Genomlysningen är därmed inte heltäckande, men genomförd på ett sådant sätt att det kan konstateras att de brister som identifierats har förekommit. När intervjuade personer beskrivit hur risker hanterats har dessa beskrivningar följts vidare uppåt och åt sidan i organisationen där det varit möjligt, vilket har möjliggjort en bredare verifiering av mönster utan att vara en fullständig kartläggning av alla riskflöden. Det innebär också att genomlysningen speglar de delar av organisationen och de situationer som intervjuade personer haft insyn i. Det finns sannolikt fler perspektiv och arbetssätt som inte omfattas här.

Genomlysningen säger inte att de identifierade bristerna har varit konstanta eller systematiska under hela införandeprocessen. Införandet har pågått under mycket lång tid. Personer och funktioner har bytts och det har hunnit genomföras flera omstruktureringar av såväl programmet som linjeorganisationen. Det är troligt att dessa förändringar i sig har påverkat förutsättningarna för riskhantering. Vissa reflektioner kring detta görs där det är relevant, men genomlysningen avgränsas till att beskriva hur riskhantering faktiskt fungerade under de delar av införandet som intervjuerna belyser.

### Definitioner och begrepp

Inom riskmanagement finns vedertagna begrepp som används även i den här analysen för att undvika missförstånd. Dessa begrepp förklaras här. I avsnittet förtydligas också några grupperingar som omnämns i genomlysningen.

**BRAG (Blue Red Amber Green) Status** är ett koncept för att markera risker i färgerna blå (omhändertagen), röd (mycket allvarlig), gul (medel allvarlig) och grön (mindre allvarlig).

**Candos** är ett dosexpedieringssystem som Millennium integrerades med. Strax innan driftstart ersattes Candos med CanS, efterföljaren av samma leverantör.

**Changeprocessen** var Program Millenniums process för att hantera ändringsbegäran.

**Co-owner** innebar inom Millennium delägare av risk på leverantörens sida, men även vice-versa.

**CR (Change Request)** är en förändringsbegäran mot omfång eller tidplan som på ett formaliserat sätt ska tas omhand inom en organisation eller projekt.

**End-to-end-tester** är ett steg i Oracles process för kvalitetssäkring. Det syftar till att testa patientens resa genom systemet så verklighetstroget som möjligt, det vill säga inklusive användning av integrationer etcetera så långt som möjligt i testsystemet.

**Enterprise Risk Management (ERM)** är ett heltäckande tillvägagångssätt för att identifiera, bedöma och minska risker som kan påverka en organisations mål.

**Hand-over** betyder överlämning från en instans till en annan, till exempel från programmet till förvaltningsorganisation, eller från en programresurs till nästa.

**Mitigering** innebär att mildra, förminska eller minska effekten av en identifierad risk.

**”Next action owner”** är personen som ansvarar för nästa åtgärds- eller uppföljningsaktivitet kopplat till risken.

**PMO (Project Management Office)**, är en central enhet inom en organisation som har till uppgift att stödja och samordna projektverksamheten.

**Risikörfattare** är personen som registrerar en risk i riskloggen.

**Riskmanager** är en person som på uppdrag av (program)chef eller projektledare ansvarar för riskmanagement i en organisation, ett program eller projekt.

**Risikägare** är personen som ansvarar för att risken blir omhändertagen.

**Regional Särskild Organisation (RSO)** var en tillfällig organisation som startades inför driftstarten av vårdinformationssystemet Millennium i syfte att på regional nivå säkerställa att akut vård och vård som inte kan anstå fungerade, åstadkomma regiongemensam lägesbild och, efter 15 november, verkställa och säkra återinförandet av tidigare system. Uppdraget avslutades 26 november 2025.

**Stakeholder** är en intressent (det kan vara en person, grupp eller organisation) som påverkas eller kan påverkas.

**Strategiska riskgruppen (SRG)** var en del av programledningen för programmet tillsammans med riskmanagers som tog beslut om vilka åtgärder som skulle vidtas baserat på mitigeringsplanen i risk- och problemloggen för riskerna med högsta riskvärdet. SRG skulle även följa upp att mitigeringen hade önskat effekt.

**Styrgrupp** i detta dokument avser antingen FVM-programmets styrgrupp (före 2022) eller Program Millenniums styrgrupp (efter 2022). Om andra styrgrupper avses så är det explicit förklarat.

**Tollgates** är fördefinierade beslutspunkter i programmet där man granskar om uppsatta milstolpar och resultat är tillräckligt uppfyllda för att gå vidare till nästa fas i programmet.

**Workarounds** är att hantera eller mitigera risk eller hinder genom att arbeta runt det. Exempelvis när en teknisk funktion inte kunde levereras ersattes den med en manuell process.

**ÖGA (ÖverGångsArkitektur)** är ett program som startades ungefär samtidigt som FVM övergick till Millennium och omfattade alla projekt och initiativ inom koncernstab digitalisering som låg utanför programmet och som behövdes för att införa Millennium.

## 4. Riskhantering i genomlysningen

I grunden syftar riskhantering till att identifiera, värdera och hantera risker som kan påverka verksamhetens mål, säkerhet och kontinuitet. Detta kapitel förtydligar hur begreppet riskhantering används i genomlysningen.

### 4.1 Vad som avses med riskhantering

I denna genomlysning omfattar riskhantering både programmets formella processer och den faktiska praktiken i styrning och ledning. Begreppet inkluderar därför:

- hur risker identifierades och värderades,
- vilka möjligheter till samlad riskbild som funnits,
- hur risker kommunicerades och eskalerades,
- vilka formella och informella vägar som användes,

- hur ansvar för risker togs i program, införandeprojekt och linjeorganisation.

Det innebär att riskhantering inte begränsas till Program Millenniums risklogg eller riskmöten. Analysen inkluderar även linjeeskaleringar, rapportering i styrande forum, direktkontakter med programledning, risk- och konsekvensanalyser och eskalering i form av skrivningar.

## 4.2 Varför ett övergripande riskperspektiv är viktigt

Införandet av en ny vårdinformationsmiljö eller större verksamhetsutveckling är ett långvarigt och komplext förändringsarbete. Under sådana förutsättningar förändras risker över tid, förstärks av beroenden och kan få bäring på flera områden samtidigt. Ett exempel är att en teknisk risk kan utvecklas till en patientsäkerhetsrisk när den påverkar vårdens arbetssätt, eller att organisatoriska beslut kan förändra riskbilden snabbt.

Traditionell riskhantering fångar ofta enskilda risker inom en sektor eller ett projekt, men ger inte en samlad helhetsbild. Det kan skapa fragmentering, otydligt ansvar och svag koppling mellan risker, beslut och konsekvens.

## 4.3 Enterprise Risk Management (ERM)

Enterprise Risk Management (ERM) är ett etablerat angreppssätt som integrerar riskhantering i styrning och beslutsfattande. I praktiken innebär ERM att:

- riskhantering fungerar likartat i linje, program och projekt,
- samband mellan risker synliggörs,
- ansvar och mandat tydliggörs,
- risker används aktivt som underlag för beslut och styrning,
- riskbilden hålls samman över tid,
- koppling till risk från ”lägre” nivå upp till beslutsfattande möjliggörs.

För en organisation av VGR:s storlek och komplexitet finns förutsättningar att dra nytta av ett mer samlat arbetssätt med risk.

## 4.4 Riskhantering i denna genomlysning

I de inledande intervjuerna framkom ett antal återkommande beskrivningar av brister i riskhanteringen. Dessa har strukturerats i tio riskkategorier som därefter använts som analytiskt ramverk i genomlysningen. Kategorierna har verifierats genom intervjuer och tillgängligt material (kapitel 5) och ligger till grund för de konkreta exempel och förbättringsförslag som redovisas senare i rapporten.

Tabell 1. Beskrivning av riskkategorier

Riskkategori	Beskrivning
<b>1. Avsaknad av samlad helhetsbild</b>	Brist på en samlad riskbild som fångar in "alla" perspektiv/riskområden som exempel ett införande av nytt system eller arbetssätt kan kräva eller som kan ha beroenden till varandra (exempel informations säkerhetsrisk som också är en patientsäkerhetsrisk)
<b>2. Bristande riskeskalering och transparens</b>	Risker identifieras lokalt men eskaleras inte vidare till (rätt) program- eller ledningsnivå.
<b>3. Tystnadskultur och undvikande av obekväma risker</b>	Risker undviks för att inte skapa konflikt, hota framdrift eller nå ledningen.
<b>4. Oklart riskägarskap och ansvar för konsekvenser</b>	Risker "ägs" formellt men inte praktiskt – otydligheter i beslutsmandat och ansvar mellan program och linjeorganisation.
<b>5. Svag koppling mellan risk och beslut</b>	Riskbedömningar saknas eller används inte vid beslut.
<b>6. Fragmenterad riskhantering mellan nivåer och projekt</b>	Riskhantering sker i separata strukturer utan samordning.
<b>7. Strukturella hinder i riskprocessen (felaktig processdesign)</b>	Processen för riskhantering är för tung, komplex eller byråkratisk för att fungera. Risker fastnar i flödet. Brister i kopplingen mot andra processer.
<b>8. Otillräcklig objektivitet i riskhanteringen (risker styrs för utseende eller kontroll)</b>	Risklistor hanteras för att det ska se bättre ut, inte för att spegla verkligheten.
<b>9. Normalisering av kända risker ("medvetet ignorerade risker")</b>	Risker är kända men hanteras inte – man "tar" dem informellt utan beslut.
<b>10. Bristande integration av programmets riskprocess med övriga VGR</b>	Olika risklistorna överlappar varandra. Man förlitar sig på att andra registrera risken hos sig, så man registrera inte i egen risklista. Likaså kan otydligheten i var man ska registrera göra att man låta bli.

## 5. Resultat per riskkategori

Nedan redovisas resultatet av den genomförda analysen.

Utifrån respektive riskkategori beskrivs specifika delar i den framtagna riskhanteringsprocessen som, om de hade fungerat som avsett, hade omhändertagit eller lindrat konsekvenserna av en eller flera av de identifierade riskkategorierna.

Därefter redovisas orsaker till att det brustit i processen och vad som ej fungerat utifrån vad som framkommit i intervjuerna och insamlat material. Vissa orsaker är återkommande i flera riskkategorier. Ett eller flera exempel ges inom varje kategori, i vissa fall är det exempel som även hör hemma inom flera andra riskkategorier.

## 5.1 Avsaknad av samlad helhetsbild

För att kunna ha en samlad helhetsbild över risker kopplade till införandet behövde såväl Program Millennium (och innan dess FVM-programmet), linjeorganisationen, leverantören som berörda samverkansparter vara involverade. Möjligheten till detta påverkades av omstruktureringen i oktober 2022, då FVM-programmet ersattes av Program Millennium. Program Millennium fick det övergripande ansvaret att leverera systemet enligt avtal och tidplan, medan ansvaret för att samordna införandeansvariga och utveckla vårdens processer lades på hälso- och sjukvårdsutvecklingsdirektören. Denna ansvarsfördelning innebar att införandeprojekten, såsom vid Närhälsan och Södra Älvsborgs Sjukhus (SÄS), agerade som separata projekt med egna styrgrupper och eskaleringsvägar på förvaltningsnivå. Programledningen uppfattade inte att det fanns någon tydlig förväntan på att Program Millennium skulle hantera förvaltningarnas verksamhetsrisker, utan att dessa hanterades inom respektive linjeorganisation och verksamhetsprojekt.

Programmet var samtidigt beroende av IT-leveranser där ansvaret för regiongemensam utveckling och tekniska förutsättningar låg hos digitaliseringsdirektören. Digitaliseringsstaben bemannade Programledningsgruppen i Program Millennium med en utsedd funktion, i syfte att samordna svar och säkerställa att VGR:s behov tillgodosågs.

Viss samordning fanns från programmet för att kunna fånga upp risker kopplat till systemet och det nya uppdraget med införandeprojekten. Men separationen av projekt innebar i realiteten separata uppdrag och separata eskaleringsvägar. Detta skapade en "gråzon" mellan programmets risker och lokala projektrisker, vilket ledde till parallella riskhanteringsspår utan samlad analys eller prioritering. När dessutom styrningen av dessa tekniska beroenden, och därmed även risker som programmet var beroende av inte styrdes av programmet, saknades en tydlig helhetsstyrning som kunde samla alla risker. Endast inom Program Millennium har det kunnat identifieras en formell riskhanteringsmodell som sträckte sig upp till styrgruppen inom Programmet.

Sammankoppling mellan programmet, de lokala införandeprojekten och övriga ansvarsområden som flyttades till koncernkontoret återfinns i styrgruppen för hälso- och sjukvårdens digitalisering. Denna grupp, ledd av regiondirektören, hade ansvar för övergripande prioriteringar och vägvalsfrågor kopplade till digitaliseringen utifrån en sammanhållen hälso- och sjukvård. Detta var den första instansen där en samlad bild över Program Millenniums uppdrag, införandeprojektens framdrift, koncernstab digitaliserings och strategiska hälso- och sjukvårdsutvecklingsstabens uppdrag var möjlig.

Utifrån den här genomlysningen har det inte varit möjligt att bedöma om riskhantering och eskalering inom de olika ansvarerna (exempelvis hälso- och sjukvårdsutvecklingsstaben, införandeprojekt, koncernstab digitalisering), som potentiellt hade påverkan på införandets resultat, har skett och rapporterats i samma mängd, på samma sätt och/eller om någon sammanvägd riskbild utifrån alla perspektiv är gjord i styrgruppen.

Det har inte heller varit möjligt att bedöma om de risker och varningssignaler som eskalerades till styrgruppen och/eller i linjen till direktörer, från till exempel medarbetare och fackliga organisationer, ingick i en samlad riskbild och riskbedömning i styrgruppen.

## **5.2 Bristande riskeskalering och transparens**

Riskeskalering innebär att risker som identifieras lokalt ska lyftas till rätt ledningsnivå för att de ska kunna bedömas, prioriteras och åtgärdas utifrån organisationens samlade riskbild. Program Millennium hade tidigt identifierat riskeskalering som ett potentiellt problemområde och etablerade därför ett antal åtgärder för att öka transparensen och möjliggöra systematisk hantering. Bland dessa fanns en gemensam risklista tillgänglig för samtliga programdeltagare, utsedda riskägare och ”next action owners” hos respektive part (VGR och Oracle), fastställda uppföljningsdatum med aktiv bevakning från risk managers, faciliterade risköppningsmöten för att säkerställa korrekt informationsunderlag samt krav på konsekvensbeskrivningar när risker inträffade.

Trots dessa insatser visar den genomförda analysen att riskeskaleringen inte fungerade som avsett och att transparensen inte upplevdes som tillräcklig. Bristerna kan huvudsakligen kopplas till fyra mönster:

- Det uppstod otydlighet till följd av delat ansvar. Modellen med två riskägare – en hos VGR och en hos Oracle – fungerade i enklare ärenden men brast vid mer komplexa risker. Ett tydligt exempel är Risk 658 (FHIR API), bilaga 1, där Oracle var åtgärdsansvarig och VGR:s chefarkitekt var riskförfattare och co-owner. Trots långdragna problem i ärendet deltog Oracles riskägare inte i de dokumenterade mötena. Avsaknaden av deltagande ledde inte till några styrsignaler eller konsekvenser. Detta innebar att den VGR-ansvarige i praktiken bar ansvaret ensam, vilket minskade möjligheten att påverka progress och lösning.
- Det saknades tydliga kommunikationsvägar från programmet ut mot berörda verksamheter. Många risker hade konsekvenser för verksamheter/enheter utanför programmet, men det saknades en gemensam process för hur verksamheterna skulle informeras eller involveras. Programdeltagare fick själva avgöra vem de skulle kontakta, vilket ibland resulterade i felaktiga antaganden om riskvärde, sannolikhet eller lämplig mitigering. Ett exempel är Risk 847 (Medanets/LOA3-integration), bilaga 2, som hanterades internt i programmet och stängdes efter lyckat test, trots att SÄS samtidigt uttryckt att de inte kunde acceptera lösningen. Detta gav upphov till en separat risk, Risk 938, bilaga 2, som öppnades samma dag av den lokala integrationsprojektledaren. Trots att risken uppmärksammats på flera håll, nåddes inte en regiongemensam bild över riskerna förrän sent i processen.
- Riskprocessens komplexitet och tyngd bidrog till att risker inte eskalerades i tid. Riskprocessen uppfattades av många som administrativt omfattande och tidskrävande, vilket ledde till att risker ”valdes bort” och hanterades enbart lokalt trots att de hade potentiellt regional påverkan. Vissa risker eskalerades aldrig, andra för sent för att möjliggöra reell mitigering.
- Avgränsningen mellan programmet och de lokala införandeprojekten innebar att strukturella hinder uppstod. Efter förändringen från FVM till Program Millennium och uppstart av de lokala införandeprojekten saknades insyn i varandras riskregister. De lokala projekten uppmanades att behålla sina risker i egna listor. Ett återkommande exempel är från SÄS som försökte registrera risker i programmets struktur men instruerades att avstå. Detta ledde till parallella riskhanteringsspår utan samlad analys eller prioritering.

Utöver dessa strukturella och kommunikativa brister visar analysen att risker ofta stängdes eller sänktes i värde utan att den person som identifierat risken informerades eller fick möjlighet att bidra med sammanhang eller konsekvensbedömning. Detta innebar att viktig kontext aldrig nådde de nivåer där beslut fattades. En återkommande iakttagelse är att risker stängdes med hänvisning till workarounds eller antaganden om att ”det kommer fungera vid start”, trots avsaknad av verifierade underlag. Sammantaget medförde detta att riskvärderingar i flera fall inte återspeglade den faktiska riskexponeringen, vilket försvagade både transparensen och möjligheten till effektiv riskstyrning.

### **5.3 Tystnadskultur och undvikande av obekväma risker**

Tystnadskultur och undvikande av obekväma risker innebär att risker inte lyfts, förskönas eller fördröjs av rädsla för konflikt, påverkan på framdrift eller oro för att nå ledningen.

I intervjuerna framkommer återkommande upplevelser av att vissa risker inte ansågs lämpliga att lyfta vid givna tillfällen, eftersom de kunde uppfattas som hinder för tidplanen eller ge signaler om bristande kontroll. Kommentarer som ”vi ville inte lyfta det nu”, ”det kommer att lösa sig vid Go Live” och ”det skulle bara bromsa” lyfts i flera intervjuer. Detta trots att det formellt fanns strukturer som borde ha synliggjort risker – såsom en gemensam risklista, en övergripande styrmodell samt införandeprojekt som följde samma riskhanteringsmetodik som programmet, inklusive BRAG-klassificering.

I KPMG:s granskning uttrycks också upplevelser av slutenhet och tystnadskultur i samband med Millennium-införandet där obekväma risker inte alltid fördes fram. Detta bedöms ha påverkat såväl arbetsmiljö som kvaliteten i de beslut som fattades inför driftstart negativt.

Analysen visar att flera faktorer bidrog till att risker inte hanterades öppet eller strukturerat:

- Avgränsningen mellan programmet och de lokala införandeprojekten gjorde att risker hanterades parallellt utan transparens.  
Efter omställningen från FVM till Program Millennium 2022 blev gränsen mot förvaltningarnas införandeprojekt tydligare. Många

projekt saknade åtkomst till programmets ytor och riskregister, och endast enstaka personer – ofta med tidigare programmerfarenhet – kunde ta del av materialet. Införandeprojektet på SÄS lyfte flera risker lokalt som motsvarade eller överlappade risker som samtidigt fanns öppna i programmets riskregister, såsom risker kopplade till Candos integrationen, schemamallar och mätvärdesöverföring. Avsaknaden av insyn och gemensam hantering försvårade möjligheten att skapa en regiongemensam riskbild och att nå samsyn kring mitigeringsnivåer.

- Det saknades fungerande arbetssätt för risker som berörde parter utanför den egna organisationen.  
Varken programmet eller införandeprojekten hade en etablerad process för risker där konsekvenserna låg hos en extern aktör, eller där mitigeringen krävde insatser utanför den egna verksamheten. Ett tydligt exempel är SÄS införandeprojekt, där projektledare och teknikrepresentanter beskriver att åtkomst till programmets ytor inte gavs förrän någon vecka före driftstart, trots att deras arbete var direkt beroende av programmets leveranser. Detta minskade möjligheten till gemensam problemförståelse och bidrog till att risker inte kunde lyftas tidigt.
- Olika typer av risker hanterades i skilda forum, vilket försvårade helhetsbedömningen.  
Kommersiella, legala, kliniska och tekniska risker lyftes och bedömdes i olika sammanhang trots att de ofta var sammanflätade och ömsesidigt beroende. Detta medförde att ingen aktör hade full överblick över den samlade riskexponeringen och att vissa risker föll mellan strukturerna.
- Beskrivningar tyder på att statistiken gällande risker ibland prioriterades högre än att riskhanteringsprocessen gav faktisk kontroll.  
I intervjuer beskriver flera personer att högt värderade eller obekväma risker ibland hanterades så att statusen skulle framstå som acceptabel snarare än att åtgärderna skulle vara tillräckliga. Detta påverkade både riskvärdering och eskalering.
- Brister i riskhanteringsprocessens legitimitet innebar att medarbetare i vissa fall slutade lyfta risker eller sökte alternativa vägar.  
När risker inte togs emot, hamnade mellan olika ansvariga forum eller stängdes utan faktisk mitigering minskade benägenheten att formellt registrera dem. Vissa försökte i stället föra fram risker informellt eller genom parallella kanaler när de upplevde att ordinarie process inte hade avsedd effekt.

- Den beskrivna tystnadskulturen innebar att allvarliga och obekväma risker ibland eskalerades snabbt för att därefter bli liggande utan åtgärd.

Flera exempel visar att allvarliga risker fördes upp till strategiska forum som konstaterade att risken "inte får inträffa", men där ingen aktiv roll togs i mitigeringen. I andra fall stängdes risker genom att planer fastställdes eller förväntningar uttalades, snarare än att faktiska leveranser säkerställdes. Något som förvärrades av tidspress och behovet att hålla tidplan inför driftstart.

Ett särskilt tydligt exempel på bristande öppenhet och ovilja att involvera relevant kompetens gäller hanteringen av funktionalitet inom transfusionsmedicin. När en medarbetare sökte stöd från labsamordnare – med både regionalt administrativt uppdrag och klinisk expertis – för att bedöma en funktion som inte uppfyllde vare sig verksamhetens behov eller avtalade SKA-krav, fick personen tillrättavisning för att ha "gått utanför programmet". Trots att programmets arbetsgrupp saknade kompetensen för att göra en korrekt bedömning skulle externa sakkunniga inte involveras. I efterhand framstår detta som ett uttryck för den tystnadskultur som beskrivs i KPMG:s rapport: obekväma risker och avtalsavvikelser skulle inte lyftas brett, och verksamhetens röst begränsades i ett läge där patientsäkerhet och funktionalitet borde varit styrande.

Ett annat exempel är när delprojekt Vårdklient påtalade risken för att inte hinna bli klar till tänkt datum och utbildningsstart, eskalerades situationen i koncernstab digitalisering. IT-chefen involverade sig och säkrade att alla nödvändiga resurser blev tillgängliga samtidigt som det jobbades på en eventuell plan B för att minimera effekten om risken ändå skulle inträffa. Beskedet från programstyrgruppens ordförande var dock att problemet skulle lösas, det fanns inget alternativ. Med andra ord accepterades inte risken. Följden blev att projektledaren för Vårdklienten funderade på att anpassa statusrapporteringen till önskat läge (= grön) i stället för faktiskt läge då bedömningen var att det inte fanns någon nytta i att lyfta risken.

Sammantaget visar analysen att flera organisatoriska, kommunikativa och kulturella faktorer bidrog till att obekväma risker inte lyftes, inte hanterades i rätt forum eller inte blev föremål för faktisk mitigering. Det påverkade både transparens, riskkvalitet och möjligheten att fatta välgrundade beslut inför driftsättningen.

## 5.4 Oklart riskägarskap och ansvar för konsekvenser

Oklart riskägarskap innebär att risker formellt tilldelas en ägare men att det i praktiken saknas mandat, ansvar eller förutsättningar för att driva mitigerings- och bärande konsekvenserna. Under införandet av Millennium förekom återkommande situationer där risker hade en utsedd riskägare och "next action owner", men där ingen aktör fullt ut tog ansvar för eller ägde de faktiska konsekvenserna om risken skulle inträffa. Detta speglas i uttryck såsom "riskägare utan mandat" och "risker som inte följs upp", vilka återkommit i intervjuerna samt i material från riskloggar och utvärderingar efter driftstoppet.

Formellt hade programmet flera strukturer på plats: en gemensam risklista på programmets portal, riskägare från både VGR och Oracle samt definierade uppföljningsdatum. Trots detta visar genomlysningen att dessa strukturer inte fick önskad effekt, och att ansvarsfördelningen brast av flera skäl:

- **Delat ansvar - en återkommande källa till otydlighet.**  
Modellen med två riskägare – en från VGR och en från Oracle – gav ibland god transparens, men brast regelmässigt vid mer komplexa risker. I Risk 658 (FHIR API), bilaga 1, saknades exempelvis aktivt deltagande från Oracles riskägare vid riskmöten, vilket gjorde att ansvaret i praktiken föll på VGR:s medarbetare trots att det endast var Oracle som kunde åtgärda risken. Avsaknaden av engagemang ledde inte till några styrsignaler eller konsekvenser, vilket visade att mandatet inte motsvarade det formella uppdraget.
- **Betydande utmaningar uppstod när den faktiska riskägaren inte fanns inom programmet.**  
Initialt försökte programmet sätta rätt sakägare – eller någon nära dennes verksamhet – som riskägare. Det var dock ofta svårt då beslut och åtgärder låg utanför programstrukturen. Med tiden övergick arbetet till att i stället utse riskägare inom programmet även när dessa saknade rådighet över riskens utfall. Exempelvis fick Risk 144 (centralisering av tidbok), bilaga 3, en riskägare hos Oracle trots att beslutet att centralisera verksamhetsprocesser inom området inte låg hos leverantören eller ens i programmet. Ett annat exempel är Risk 574 (ingen utskriftsfunktion), bilaga 4, som tilldelades en teknikansvarig inom programmet trots att mitigerings- och bärande konsekvenserna låg hos printteamet i

koncernstab digitalisering. I båda fallen saknade riskägaren praktiska möjligheter att påverka riskens utveckling.

- I praktiken fanns det få konsekvenser när riskägare inte utförde sina åtaganden.  
Exempel från riskloggen, bilaga 4, visar att bristande uppföljning, uteblivet deltagande eller fördröjd mitigering sällan ledde till åtgärder från programledningens sida. Detta försvagade både ägarskap och incitament att driva risker framåt.
- Konsekvensförståelsen framstår ofta som otillräcklig  
Risker kvantifierades från ett till fem, men utan att den faktiska verksamhetspåverkan tydliggjordes. Risk 66, bilaga 5, (LoN-verktyget som väckte dataskyddsrisker, men som behövdes för viktiga övervakningsfunktioner), hade ett högt riskvärde men begränsad progress över flera år, delvis för att vidden av konsekvenserna inte fullt ut förstås trots kritisk koppling till leverantörens prestandatester. Samtidigt visar Risk 1 (möjliga missförstånd och fel på grund av engelska/svenska språkbruk), bilaga 6, hur en initialt lågklassad risk som stängdes efter en vecka, senare visade sig ha betydande påverkan på användbarhet, utbildning och driftsättning.
- Ansvarsfördelningen innebar att risker i vissa fall delades upp i mindre delar utan att någon tog ansvar för helheten  
Ett tydligt exempel är hanteringen av ordinationsunderlaget inför driftstart, där olika komponenter – utskrift, signering, flöden i primärvården och beroenden till andra processer – separerades i delrisker och bedömdes var för sig. Detta resulterade i att den samlade risken inte synliggjordes och att ingen aktör tog ägarskap för helheten, trots att verksamheten lyfte att funktionaliteten inte var acceptabel.

Sammanfattningsvis visar analysen att bristande mandat, fragmenterat ägarskap, frånvaro av konsekvenser vid utebliven riskhantering samt otillräcklig förståelse av riskernas verkliga påverkan sammantaget bidrog till att flera centrala risker inte hanterades effektivt. Detta ledde till fördröjd mitigering, undervärderade risker och en bristande koppling mellan ansvar och konsekvens – vilket i sin tur minskade programmets förmåga att styra riskexponeringen på ett ändamålsenligt sätt.

## 5.5 Svag koppling mellan risk och beslut

Analysen visar att kopplingen mellan risker och beslut i Program Millennium var svag och att riskbedömningar inte alltid utgjorde ett reellt

underlag för de beslut som fattades. Trots att flera förbättringar gjordes under programmets gång – såsom en mer avskalad riskprocess med fokus på identifiering och samsyn samt en förbättrad koppling mellan riskprocessen och changeprocessen – kom programmet inte i mål med att integrera riskinformationen i beslutsfattandet på ett konsekvent sätt. Detta gav upphov till en situation där riskernas påverkan på programstyrning, prioriteringar och tidsplaner ofta blev begränsad.

I intervjuerna har det bland annat framkommit att leverantörens rekommendationer ibland vägde tyngre än den egna riskbedömningen, och att kvarstående risker inför driftstart accepterades trots att de inte var fullt ut mitigerade. Även förändringar i scope och design genomfördes utan att konsekvenser för befintliga risker eller nya risker analyserades i tillräcklig omfattning.

Flera faktorer bidrog till bristen på koppling mellan risk och beslut:

- **Riskprocessen upplevdes som tung och långsam.**  
Tiden mellan identifiering av en risk och dess uppförande i programledningen var ofta så lång att åtgärder inte hann genomföras. Risk 279 (osäker användning av root-konto), bilaga 7, är ett exempel på en risk som hanterades i flera forum under lång tid utan att riskägare tog tydlig handling, vilket ledde till en utdragen ”långbänk” snarare än beslutad lösning.
- **Beslutsnivån styrdes nästan uteslutande av riskvärdet, inte av praktisk brådska eller samlade konsekvenser.**  
Även om modellen medgav att tidskritiska risker kunde justera sannolikhet eller påverkan, skedde detta sällan i praktiken. Det innebar att risker som borde ha eskalerats tidigt inte nådde programmets beslutsforum i tid, vilket framgår i bilaga 8 (brister i kravuppfyllnad kring Loggtjänster) där risken identifierades tidigt i integrationsprojektet, men tidig eskalering fungerade inte trots flera öppnade risker. En framgångsrik tidig eskalering hade möjliggjort en fullständig lösning innan driftstart.
- **Beslut fattades i vissa fall utan att helheten var tillräckligt känd eller analyserad.**  
I vissa fall framkom det först långt efter beslutet att nya risker introducerats genom själva beslutet. Bilaga 9, illustrerar detta, där beslutet att exkludera privata vårdgivare från första driftsättningen skapade beroenden kring labbflöden mellan SÄS och privata aktörer. Detta ledde senare till Risk 860 (unsolicited results), bilaga 9, som talar

om behov att ändå inkludera vissa privata vårdgivare, som i sin tur bidrog till problematiken kopplad till risken om utmaningen att hålla tidplanen för delprojekt Vårdklient, bilaga 10. Med en mer systematisk riskkonsekvensanalys hade dessa frågor kunnat identifieras och hanteras innan beslutet fattades.

- Kopplingen mellan riskprocessen och changeprocessen visade sig inte vara tillräckligt robust.  
Även om changeprocessen mot slutet tog hänsyn till riskbedömningar uppstod problem när en change request (CR) öppnades som del i en mitigering. I vissa fall stängdes risken så snart CR skapats – trots att CR:n endast omfattade en del av mitigeringen eller levererades i flera steg. Exempel CR 347 och Risk 688, bilaga 11, handlar om att hantera avvikelser i informationen mellan Millennium och Inera som uppstod då meddelanden som inte levererats på grund av tekniska problem inte sändes om. Oracle åtgärdade det i två steg, den första rättningen som lindrade problemet kom innan driftstart, den fullständiga lösningen kom först året därpå. Exemplet visar därmed hur en risk stängdes i samband med att CR:n genererades, trots att den fullständiga mitigeringen levererades först året efter driftstart. Det innebar att delar av risken implicit accepterades utan formellt beslut.
- Beslut fattades utan att verksamhetsbehov eller praktiska konsekvenser var tillräckligt genomlysta.  
Ett tydligt exempel är hanteringen av ordinationsunderlaget, där brister i funktionalitet – som verksamheten påtalade – inte åtgärdades, utan kom att hanteras med lathundar och utbildningsinsatser. Besluten grundades ofta på leverantörens antaganden och jämförelser med andra regioner. Detta visar på ett återkommande mönster där risker inte utgjorde primärt beslutsunderlag, utan där beslut i stället styrdes av tidplan, framdrift och begränsade bedömningsunderlag.

Sammantaget visar analysen att kopplingen mellan riskhantering och beslutsfattande inte var tillräckligt integrerad. Långsamma processer, en snäv styrning via riskvärden, otillräcklig helhetsanalys, brister i harmonisering mellan risk- och changeprocess samt beslut som togs utan full förståelse för verksamhetskonsekvenser bidrog till att flera risker accepterades – explicit eller implicit – utan att vara tillräckligt genomarbetade. Detta försvagade programmets förmåga att fatta robusta beslut inför driftstart och ökade den faktiska riskexponeringen.

## 5.6 Fragmenterad riskhantering mellan nivåer och projekt

Analysen visar att riskhanteringen i Program Millennium präglades av fragmentering mellan nivåer, projekt och organisatoriska gränser. Även om vissa risker registrerades i programmets risklogg och hanterades enligt formell process, blev många risker antingen aldrig registrerade, hanterades enbart lokalt eller föll mellan strukturer. Det innebar att programmet saknade en sammanhållen riskbild och att viktiga risker inte adresserades på rätt nivå.

Det fanns positiva inslag, såsom projektkontorets faciliterade risköppningsmöten som syftade till att tydliggöra vilka delar av organisationen som berördes av en risk. Trots detta utvecklades flera mönster som bidrog till att riskhanteringen blev fragmenterad:

- Konceptet med riskägare innebar att risker ofta begränsades till ett område i stället för att ses i ett helhetsperspektiv.  
I komplexa risker där både teknik, verksamhet, infrastruktur och kliniska konsekvenser berördes blev riskhanteringen sektoriell och beroende av riskägarens kompetens och mandat. Bilaga 12 (ingen reservinstans bestämd), illustrerar detta tydligt: risker öppnades, stängdes och omformulerades i flera forum över flera år utan att ansvar för helheten etablerades. Riskägarskapet flyttades mellan teknikprojekt, verksamhetsrepresentanter och leverantör, men utan tydlig samlad bedömning eller samordnad mitigering. Detta ledde till parallella riskspår både inom VGR och hos Oracle.
- En brist var avsaknaden av funktionell filtrering som tydliggjorde på vilken nivå en risk hörde hemma.  
Programmets riskregister innehöll över 1 000 registrerade risker inför driftstart, men registret saknade möjlighet att sortera risker efter projekt, arbetsström eller organisatorisk nivå. Detta gjorde det svårt att få överblick och att identifiera vilka risker som krävde programledningsbeslut, vilka som hörde till lokala införandeprojekt och vilka som borde eskalerats till Regional Särskild Organisation (RSO). Denna brist, som försvårade styrning och prioritering, är dokumenterat i, bilaga 13.

- Nya riskägare tilldelades ibland risker under riskmöten trots att de inte deltog.  
Projektkontoret förmedlade därefter uppdraget, men eftersom riskägarna saknade kontext blev handover otillräcklig. Bilaga 14 (risk 288 – nödvändiga anpassningar för synskadades användning av Millennium), visar hur en risk placerades hos en person som inte längre var operativ i programmet, vilket ledde till att riskarbetet saknade aktiv drivning tills andra aktörer tog över informellt. Detta visar på en strukturell brist där riskägarskapet inte var kopplat till mandat eller faktisk förmåga att agera.
- Riskmötesprocessen var resurskrävande och långsam.  
För att samla alla nödvändiga stakeholders kunde ett öppningsmöte fördröjas i upp till två månader, vilket innebar att risker stod utan riktning eller åtgärd under kritiska perioder. Detta accentuerades av att vissa forum inte kunde samla representanter från både program, införandeprojekt och verksamhet samtidigt.
- Testprocessen utgjorde en central källa till fragmenterad riskhantering.  
De genomförda testerna speglade inte verksamhetens faktiska flöden: testare hade fel roller, testmiljöerna motsvarade inte produktionsmiljön och centrala scenarier – bland annat primärvårdens provtagningsprocesser – saknades helt från End-to-End-testerna. När nya fel upptäcktes i sen fas saknades möjlighet att registrera felrapporter eller skapa nya testfall eftersom testfasen var avslutad. Detta innebar att risker som direkt berörde användarflöden, patientsäkerhet och funktionalitet aldrig införlivades i programmets risklogg och därmed inte heller synliggjordes för programledning eller RSO. Testprocessen illustrerar hur risker föll mellan flera organisatoriska och administrativa gränssnitt – mellan programmet, leverantören, testorganisationen och de lokala införandeprojekten.

Sammantaget visar analysen att avsaknad av tydliga nivåindelningar, brist på helhetsperspektiv, otillräcklig koordinering mellan program och lokala projekt samt svag koppling mellan testresultat och riskhantering ledde till en fragmenterad och i delar ineffektiv riskhanteringsprocess. Detta minskade möjligheten att upptäcka systemrisker, att prioritera rätt åtgärder och att styra införandet mot en kontrollerad riskexponering.

## 5.7 Strukturella hinder i riskprocessen

Analysen visar att flera av bristerna i Millennium-programmets riskhantering kan kopplas till strukturella begränsningar i själva processdesignen. En tung, komplex och i delar byråkratisk riskhanteringsprocess gjorde att risker fastnade i flöden, hanterades långsamt eller inte integrerades med andra centrala styrprocesser. Detta skapade ett system där processkrav i sig blev ett hinder för att identifiera, dokumentera och åtgärda risker i tid.

Ett återkommande exempel är att risker stängdes så snart en mitigering påbörjats, även om åtgärden endast begränsade riskens påverkan eller om den formella mitigeringen bestod av en change request (CR) som ännu inte var beslutad eller implementerad. I praktiken innebar detta att risker stängdes på antaganden om framtida leveranser, snarare än på verifierade åtgärder. Detta strider mot etablerad best practice inom riskhantering där risker bör hållas öppna tills de antingen inträffat, eliminerats eller accepterats genom ett tydligt beslut. När risker stängs utan kontrollerad mitigering försämras transparensen och organisationen förlorar spårbarhet i riske exponeringen.

Det fanns positiva inslag i processen, bland annat att både VGR och Oracle hade dedikerade risk managers som drev riskarbetet över långa sträckor. Trots detta utvecklades flera strukturella hinder som påverkade riskhanterings kvaliteten.

- Riskmanagernas rekommendationer i utformningen av processen förbisågs.  
Både VGR:s och Oracles risk managers uttryckte återkommande att processens utformning inte följde vedertagen riskhanteringspraxis, särskilt avseende tidiga stängningar av risker innan mitigeringen var genomförd. Bilaga 15, visar hur denna kritik framfördes av flera sakkunniga – inklusive teknikansvarig med internationell erfarenhet av riskarbete – men avvisades av programledningen utan saklig motivering. Detta skapade en uppfattning om att statistik och mängden öppna risker vägde tyngre än faktisk transparens.
- Processen för riskmöten var tung, långsam och starkt beroende av att alla parter deltog.  
För att genomföra ett öppningsmöte krävdes ofta att både VGR:s och Oracles representanter fanns tillgängliga, vilket ledde till långa ledtider och perioder där risker saknade aktiv hantering. Denna flaskhals återkommer även i redan nämnda exempel med inte uppfyllda

Loggtjänstkraven, bilaga 8, där kritiska risker fördröjdes av processmässiga krav.

- **Processen saknade en tydlig struktur för att integrera riskhantering mellan projekt-, arbetsströms- och programnivå**  
Samtliga risker samlades i en och samma risklista, men utan funktion för att filtrera per projekt eller nivå. Det fanns ingen tydlig delegationsordning som reglerade vilka risker som skulle hanteras var, eller hur risker skulle överlämnas mellan nivåer. Bilaga 13, visar att registret omfattade över 1 000 risker inför driftsättning, men att det saknades verktyg för att identifiera vad som tillhörde vilket projekt eller vilken arbetsström.
- **Processerna var inte integrerade med omvärlden – varken med linjen, införandeprojekten eller regional särskild organisation (RSO).**  
Det var oklart hur riskstatus skulle hanteras i Tollgates, GO/NO-GO-beslut och andra regionala forum. Detta resulterade i att parallella strukturer utvecklades utanför programmet. Bilaga 16 illustrerar hur SÅS tvingades skapa en egen ”13-lista” för att fånga kritiska punkter som programmet inte upplevdes hantera tillräckligt objektivt eller transparent.
- **Testningen och arbetet med arbetsflöden utgjorde ett tydligt exempel på hur processdesignen hindrade korrekta riskbedömningar**  
Standardiserade arbetsflöden från Oracle saknade vissa verksamhetskritiska steg, och när VGR försökte utöka testfallen stoppades detta av tidplan och processregler. Eftersom felrapporter måste knytas till specifika teststeg blev det omöjligt att rapportera brister som upptäcktes efter att testfall låsts. Detta innebär att risker med klinisk påverkan inte kunde dokumenteras, inte kunde hanteras och inte kunde synliggöras för programledning eller RSO. Här utgör själva processen – snarare än bristen på vilja – det strukturella hinder som förhindrade god riskhantering.

Sammantaget visar analysen att den formella riskprocessen i flera delar fungerade som ett organisatoriskt hinder i stället för ett verktyg för styrning. En komplex process, bristande koppling mellan nivåer, avsaknad av filtreringsmekanismer, utebliven integration med omvärlden samt processrelaterade begränsningar i testning och arbetsflöden gjorde att

risker inte identifierades, inte hanterades och inte följdes upp på ett ändamålsenligt sätt.

## 5.8 Otillräcklig objektivitet i riskhanteringen

Analysen visar att riskhanteringen i vissa fall påverkades av hur riskbilden skulle se ut snarare än hur den faktiskt såg ut. Detta innebar att risker styrdes, justerades eller fördelades på ett sätt som gav ett mer positivt eller kontrollerat intryck, men som inte fullt ut speglade den faktiska riskexponeringen. Fenomenet uppträdde särskilt i situationer där VGR och Oracle hade olika uppfattningar om en risk, vilket ibland ledde till att risker inte öppnades trots att behov fanns – något som skapade frustration på båda sidor. I andra fall kunde riskvärden påverkas av hur en rapport skulle tas emot, snarare än av faktisk sannolikhet och konsekvens. Det förekom även att risker flyttades mellan faser (exempelvis från PD1 till PD2) eller hanterades i interna listor för att undvika synlighet inför programledning eller GO/NO-GO-forum.

Det fanns samtidigt positiva inslag. Under det sista året inför driftsättningen deltog riskmanagers regelbundet i programledningen för att objektivt redovisa status och utveckling, och den Strategiska Riskgruppen etablerades för att ge ökad prioritet åt risker med högt riskvärde och svag progress. Trots dessa initiativ utvecklades flera mönster som bidrog till en otillräcklig objektivitet eller strategiskt styrd riskhantering.

- Ett återkommande mönster var att riskvärden i vissa fall diskuterades utifrån hur de skulle påverka programledningens möte, snarare än utifrån en objektiv bedömning.  
Inför programledningsmöten fördes ibland dialoger mellan risk managers och riskägare om huruvida riskvärdet ”behövde” vara så högt, eller om risken kunde sänkas för att undvika eskalering. Syftet var inte nödvändigtvis att förbättra riskhanteringen, utan att styra vilka risker som skulle nå programmets beslutsforum. Detta beskrivs bland annat i diskussioner kring integrationsrisker och visar ett mönster där riskvärdet anpassades efter önskat processutfall.
- Rekommendationer från risk managers om god riskhanteringspraxis förbisågs ibland.  
Som framgår av intervjuer, se bilaga 15, framförde både VGR:s och Oracles risk managers återkommande att programmet inte borde stänga

risker innan mitigeringen var genomförd. Trots tydliga hänvisningar till best practice avvisades dessa rekommendationer av programledningen, vilket ökade risken för att statistik – såsom antal öppna risker – blev styrande för hanteringen.

- Den Strategiska Riskgruppen fokuserade i vissa fall på att uppnå en "nästa åtgärd" för att kunna stänga risken, snarare än att säkerställa att åtgärden faktiskt genomfördes

Detta är tydligt i redan omnämnda exempel kring Loggtjänsternas brister bilaga 8, där risker kopplade till loggtjänster hanterades genom att planera framtida åtgärder snarare än att säkerställa leverans eller mitigering. Det hade som slutlig konsekvens att endast tre veckor innan driftsättningen beslutade VGR ensidigt att backa från att driftsätta integrationen med Inera och i stället jobba med manuella rutiner. I praktiken stängdes risker trots att faktiska problem kvarstod och i vissa fall först blev fullt synliga inför eller efter driftsättning.

- Riskbilder reducerades genom uppdelning, vilket möjliggjorde att risker kunde stängas eller ges lägre riskvärde trots att helheten kvarstod.

I arbetet med ordinationsunderlaget delades den samlade utskrifts- och arbetsflödesproblematiken upp i flera delrisker. Var för sig kunde dessa värderas som begränsade, men den faktiska samlade konsekvensen – som verksamheten lyfte – framgick inte längre i riskloggen. I kombination med tidspress och mål om att begränsa antalet öppna risker inför driftstart ledde detta till en riskbild som inte reflekterade verkliga förutsättningar.

Sammantaget visar analysen att delar av riskhanteringen påverkades av önskan att skapa en mer positiv eller kontrollerad bild av läget. Justerade riskvärden, selektiv registrering, uppdelning av risker, bristande efterlevnad av rekommenderad praxis och forum där planering ersatte faktisk mitigering bidrog till en riskhantering som i vissa delar blev mer styrd av utseende än av faktisk risk. Detta försvagade programmets förmåga att fatta välgrundade beslut och ökade den faktiska risken inför driftsättningen.

## 5.9 Normalisering av kända risker

Normalisering av kända risker innebär att risker som är välkända och återkommande successivt tappar uppmärksamhet, prioritet och

handlingskraft. I stället för att fatta ett tydligt beslut om acceptans – och därmed skapa transparens – blir risken kvar som en ”långbänk”, där den rapporteras men inte aktivt hanteras. I intervjuer beskriver flera personer att sådana risker ofta hanterades med uttryck som ”vi visste men körde ändå” eller ”det får vi ta sen”. Det innebär att riskerna varken stängs genom faktisk mitigering eller genom ett formellt beslut om acceptans.

Det fanns positiva inslag i arbetet. Denna typ av risker mörkades sällan formellt – de förblev oftast öppna i riskloggen – och risk managers hade rutiner för att påminna om uppföljningsdatum samt redovisade periodvis hur länge risker hållits öppna. Trots detta utvecklades flera mönster som gjorde att risker med betydande påverkan normaliserades över tid:

- **Mänskliga beteenden och organisatorisk tröghet gör att långvariga risker successivt tappar fokus.**  
När en risk inte kan lösas inom rimlig tid, eller när ansvar och påverkan ligger utanför den egna rollen, är det naturligt att risken förlorar prioritet. Detta syns i flera av de exempel som redan analyserats, såsom bilaga 9, Vårdklient, eller bilaga 15, Reservinstans, där risker återkommande flyttades fram utan att åtgärdas.
- **Under perioder saknades det systematisk uppföljning från riskmanagers för risker som inte var prioriterade.**  
Även om riskmanagers arbetade aktivt med många risker är det tydligt att vissa risker – särskilt de med lägre politisk uppmärksamhet eller utan omedelbara konsekvenser – inte följdes upp i samma omfattning. Flera riskloggar visar långa tidsintervall utan anteckningar, vilket illustrerar hur risker kunde falla mellan cracks i processen. Redan redovisade risk 279 om osäker användning av root kontot, bilaga 7, visar att risker kunde ligga öppna i mycket lång tid utan aktiv drivning.
- **Flera risker försvann i gränssnittet mellan risk- och changeprocessen.**  
Som tidigare exemplifierats i bland annat Bilaga 9 (Exkludering av privata vårdgivare), och Bilaga 7 (Rootkonto) stängdes risker när en change request påbörjades, trots att själva mitigeringen inte var genomförd. När CR:n sedan avslogs, ändrades eller endast delvis levererades, öppnades risken inte alltid på nytt. Risken blev då i praktiken ignorerad, även om den kvarstod.
- **Fokus på de egentliga riskerna försvagades när stängning av risker prioriterades framför faktisk hantering.**  
I flera fall finns dokumentation där projektmedlemmar försökte lyfta att en risk inte var åtgärdad, men där detta inte ledde till återöppning eller

omvärdering. Bilaga 11, visar att det till och med fanns uttrycklig dokumentation om att en risk inte skulle öppnas igen, trots att mitigeringen inte levererats före driftsättning.

- Det skapades styrsignaler som förstärkte normaliseringen.

Riskmanagers fick vid ett tillfälle uppdraget att arbeta bort ”för gamla” risker. Detta blev i praktiken ett incitament att stänga risker snarare än att hantera dem. Från programledningspresentationer, se Bilaga 17 framgår att allvarliga accepterade risker inte redovisades som en del av den totala riskexponeringen, eftersom de var stängda. Därmed fick beslutsfattare en bild av att risknivån var lägre än den faktiskt var, vilket förstärkte risken för passivitet och normalisering.

Sammantaget visar analysen att normalisering av kända risker är en av de mest betydande bristerna i riskhanteringen. Långvariga risker som saknade direkt möjlighet till åtgärd tenderade att bli stående i systemet utan aktiv hantering. Avsaknad av konsekvent uppföljning, processrelaterade hinder, felaktig stängning av risker och bristande transparens kring accepterade risker gjorde att dessa risker inte integrerades i beslutsfattandet – trots att de ibland var av avgörande betydelse inför driftsättning. Detta kan i efterhand ses som en medveten ignorering av risker som borde hanterats med större tydlighet, struktur och ansvarstagande.

## **5.10 Bristande integration av Program Millenniums riskprocess med övriga VGR**

Analysen visar att en grundläggande brist i Millennium-införandet var avsaknaden av en sammanhållen riskhanteringsmodell som sträckte sig över programmet, de lokala införandeprojekten och linjeorganisationen. Risker som hade sitt ursprung i programmet men fick konsekvenser utanför programmet – eller vice versa – integrerades inte i en gemensam struktur. Detta gjorde att ansvarsfördelning, ägarskap och uppföljning blev otydligt, och att betydande risker varken hanterades eller synliggjordes på rätt nivå.

Problemet blev särskilt tydligt vid organisatoriska förändringar som gjordes och beslut som fattades parallellt med Millennium-införandet, men som inte direkt var en del av Program Millennium. I dessa fall hamnade risker ofta mellan stolarna. Antingen tog programmet ett ansvar för risker som egentligen hörde hemma i annan struktur, eller så hanterade programmet endast sin begränsade del utan att helheten omhändertogs av ansvarig instans. Resultatet blev att risker ibland upptäcktes men aldrig formellt

registrerades eftersom de inte ”passade” i programmets process eller för att de ansågs tillhöra en annan del av organisationen.

Flera försök gjordes både inom programmet och i linjeorganisationen att skapa gemensamma arbetssätt, dela risker och utveckla samarbetsytter. Bland annat fanns initiativ där projekt inom ÖGA och teknikansvarig i programmet samordnade risklistor vid sidan av programmet. Trots detta blev effekten begränsad på grund av att den övergripande strukturen saknade förmåga att binda samman riskhantering mellan nivåerna.

Flera orsaker bidrog till den bristande integrationen:

- En grundläggande förutsättning som saknades var en gemensam riskkultur och gemensamma arbetssätt. Bortsett från patientsäkerhetsområdet fanns ingen etablerad kultur i VGR som styrde hur risker skulle identifieras, värderas och hanteras tvärs över linje, projekt och program. Varje del av organisationen utvecklade sina egna risklistor, processer och definitioner. Bilaga 18, visar detta tydligt: SÄS införande projekt använde exakt samma riskmodell som programmet (inklusive BRAG-status), men trots upprepade försök togs deras risker inte in i programmets struktur. Detta innebar att två parallella riskbilder utvecklades utan att de någonsin vävdades samman.
- Ambitionen att skapa gemensamma verktyg och forum i praktiken blev begränsad till vissa perspektiv. Initiativ som gemensamma risklistor för specifika teknik- eller integrationsområden fungerade lokalt, men saknade koppling till programmets övergripande process. Detta innebar att vissa risker samarbetades kring, medan andra aldrig nådde programmets riskregister eller dess beslutsforum.
- Det saknades en naturlig eskaleringspunkt när risker föll utanför programmets ägarskap. När ett projekt eller en arbetsström insåg att de inte nådde fram med behov eller förslag fanns ingen definierad väg för att eskalera frågan vidare i organisationen. Detta bidrog till att risker fastnade i ändlösa diskussioner eller ”långbänkar”, såsom illustreras i bilagorna 1,3,7 och 8. Utan en tydlig kedja för ansvar och beslutsfattande stannade riskerna kvar i program- eller projektstrukturen även när de borde hanterats av linjen, avtalssidan, teknisk förvaltning eller RSO.

Sammantaget innebar dessa brister att programmets riskprocess inte var integrerad med regionens övriga strukturer för styrning och riskhantering. Detta ledde till parallella riskhanteringssystem, bristande transparens mellan nivåer och avsaknad av en sammanhållen riskbild för VGR som helhet. Den fragmenterade integrationen försvårade möjligheten att fatta informerade beslut, särskilt i frågor där Millennium-införandet korsade andra förändringar inom organisationen.

## **6. Reflektioner: Iakttagelser kring organisatoriska mönster**

Genomlysningen och analysen har resulterat i ett antal reflektioner och iakttagelser gällande mönster och brister i riskhanteringen i samband med Millennium-införandet, baserat på tillgängligt material och intervjuer. Gjorda iakttagelser pekar på områden där VGR kan behöva stärka sina strukturer, arbetsätt och sin kultur. Det är viktigt att notera att denna analys inte är heltäckande, utan är framtagen för att bidra till lärande och förbättring i regionens fortsatta strategiska arbete med riskhantering.

Riskhantering är i grunden ett strategiskt ledningsverktyg, inte en administrativ process. Erfarenheterna från införandet av Millennium, särskilt bristerna kopplade till avsaknad av samlad helhetsbild, fragmenterat ansvar, otydligt ägarskap och svag koppling mellan risk och beslut, understryker behovet av en organisationsövergripande riskhanteringsmodell. En sådan modell måste fungera oavsett om arbetet bedrivs i linje, program eller projekt, och den måste omfatta ett allriskperspektiv. Att hantera risker utifrån ett allriskperspektiv är nödvändigt eftersom risker sällan är statiska utan förändras, förstärks eller skiftar karaktär över tid. Dessutom är risker ofta sammanflätade, där exempelvis en informationssäkerhetsrisk också kan vara en patientsäkerhetsrisk. Vikten av en god riskhantering och risk som ett verktyg för fortlöpande styrning stärks när en förändring löper över längre tid, är omfattande och sker inom ett område där omvärlden (och därmed risk) förändras snabbt.

En organisationsövergripande riskhanteringsmodell innebär att riskhantering integreras naturligt i all styrning och beslutsfattande, vilket ger organisationen en samlad, tydlig och framåtblickande riskbild för att skydda verksamhet, patienter och uppsatta mål. Följande reflektioner bygger på denna insikt och undersöker hur VGR:s förmåga att hantera risker kan stärkas.

## 6.1 Strategiskt gap mellan program och organisation

Iakttagelserna pekar på att det fanns en brist i integrationen mellan den formaliserade riskhanteringsprocessen i Program Millennium och linjeorganisationen. Programmet utgjorde den enda instans där en kontinuerlig riskhanteringsmodell med rapportering till styrgrupp kunde identifieras.

- **Fragmentering:** De identifierade bristerna i riskhanteringen pekar på bristen i att VGR saknar en sammanhållen riskhanteringsmodell som sträcker sig över hela organisationen oberoende av linje, program och lokala införandeprojekt och/eller oberoende av typ av risk.
- **Gråzoner i Ägarskap:** Mönster som "oklart riskägarskap och ansvar för konsekvenser" och att risker delades upp i mindre delar utan att någon tog ansvar för helheten kan indikera på att det fanns otydliga mandat och en gråzon mellan programmets ansvar och linjens ansvar. Detta försvårade möjligheten att hantera risker som hade bärighet på varandra, exempelvis att en informationssäkerhetsrisk också kunde vara en patientsäkerhetsrisk.
- **Parallella Spår:** Att risker hanterades i parallella riskhanteringsspår och att programmet eller införandet var beroende av leveranser vars risker styrdes utanför programmet pekar på att det fanns strukturella hinder som försvårade en tydlig och samlad helhetsbild av riske exponeringen.

## 6.2 Iakttagelser kring ledning och beslutskultur

Ett centralt tema i genomlysningen är hur riskinformation hanterades, värderades och användes i beslutsfattandet.

- **Risk som Styrinstrument:** De upplevda bristerna i "tystnadskultur och undvikande av obekväma risker" och att obekväma risker inte lyftes pekar på att riskhantering eller att eskalera risker i vissa delar kan ha setts som ett hinder för framdrift snarare än ett verktyg för styrning.
- **Koppling mellan Risk och Beslut:** Mönstret "svag koppling mellan risk och beslut" och att beslut fattades utan fullständig riskkonsekvensanalys kan indikera på att det fanns brister i legitimiteten hos riskprocessen och att riskinformation inte alltid utgjorde ett reellt underlag för de strategiska val som gjordes.

- **Normalisering:** Att risker som var välkända och återkommande "normaliserades" och gradvis tappade uppmärksamhet kan peka på att det fanns ett behov av tydligare formella beslut om acceptans av kvarstående risker i VGR:s ledningsstrukturer.
- **Ledarskap och Kompetens:** Iakttagelsen att chefer och tekniska ledare haft formellt ansvar utan motsvarande mandat att översätta tekniska frågor till organisatoriska beslut pekar på ett glapp mellan beslutsnivå och sakkunskap. Detta kan ha försvårat möjligheten att kommunicera riskernas konsekvenser på ett sätt som gjorde dem begripliga i ledningskedjan.

## 7. Förbättringsförslag

Förslagen syftar till att omvandla riskhantering från en reaktiv, fragmenterad eller ceremoniell process till ett proaktivt och integrerat verktyg för strategisk styrning av VGR.

### 7.1 Strategisk integrering av riskhantering

- **Införande av en organisationsövergripande riskhanteringsmodell**  
VGR bör utvärdera införandet av en sammanhållen riskhanteringsmodell som ett verktyg och instrument för styrning. Modellen måste fungera oberoende av om arbetet bedrivs i linje, program eller projekt, eller i en mix av dessa, samt ur ett allriskperspektiv. Denna modell bör integreras i all styrning och beslutsfattande.
- **Gemensamt verktygsstöd för hela organisationen:**  
Inför ett gemensamt verktygsstöd för riskhantering för hela VGR. Det kan bidra till ökad transparens, minskad administration, minimera risken för att risker filtreras bort mellan olika nivåer och säkerställa trygg eskalering av risker mellan olika nivåer och typer av projekt.
- **Tydlig eskaleringsstruktur för långvariga risker:**  
Etablera en tydligt definierad eskaleringsstruktur för när risker ligger länge ("gamla risker") utan att mitigering uppnås eller utan att risken kan accepteras formellt.
- **Risk som obligatoriskt beslutsunderlag:**  
Inför en rutin där alla beslut – i synnerhet strategiska vägvalsfrågor och förändringar i omfattning – ska föregås av en riskanalys. Detta för att

logga nyintroducerade risker tidigt och säkerställa att konsekvenser för kända risker beaktas innan beslut fattas.

- Bevakning av beslut ur ett riskperspektiv: Inför förmåga där beslut bevakas ur minst ett strategiskt riskperspektiv, då nya risker som hindrar eller hotar mål kan uppstå under resans gång (i enlighet med principer som återfinns i etablerade riskhanteringsmodeller).

## 7.2 Stärkt ledarskap och kulturellt skifte

- Främjande av öppenhet och belöning:  
Driv en kulturförändring där det tydligt signaleras från ledningen att risklyft är önskvärda och ska belönas, inte tystas ned. Öppenhet ska ses som ett uttryck för ansvar, då riskhantering är ett styrmedel och inte ett hinder i beslut.
- Stärkt ledarskapskompetens:  
Stärk chefer och tekniska ledares förmåga på alla nivåer att både förstå professionens eller teknikens realiteter och omsätta dem till risk och konsekvens för att uppnå verksamhetsnytta.
- Tydligt ägarskap och konsekvensansvar:  
Tydliggör att konsekvensbedömningen måste undertecknas av den som berörs av konsekvensen, vilket minskar risken för manipulation och tydliggör ansvaret. Inrätta att konsekvenser ska uppstå om riskägare inte följer processen och sina förpliktelser.

## 7.3 Processens Robusthet och Transparens

- Tydlig riskstatus för acceptans:  
Risker som accepteras genom ett formellt beslut av ledningen bör få status "accepterad" i stället för "stängd". Detta skapar ökad transparens kring den faktiska riskexponeringen.
- Disciplinerad stängning av risk:  
Risker bör inte stängas förrän mitigeringsplanen är helt genomförd eller möjligheten att risken inträffar har försvunnit.
- Oberoende granskning och kontroll:  
Undersök möjligheten att koppla riskhanteringssystemet till en form av avvikelserapportering eller oberoende granskning, där hanteringen av specifika risker kan granskas om berörda parter känner sig otrygga