Kf §

15. Granskningsrapport om IT-verksamheten och arbetet med informationssäkerhet i Västerviks kommun

Dnr 2017/67-007

Kommunens förtroendevalda revisorer har uppdragit åt PwC att granska IT-verksamheten och arbetet med informationssäkerhet i Västerviks kommun.

I skrivelse 13 februari 2017 överlämnar revisorerna granskningsrapport från PwC samt ett utlåtande över utförd granskning.

Syftet med granskningen är att klargöra vilka eventuella områden som kommunen behöver utveckla för att uppnå en optimal IT-leverans i alla delar inklusive IT- och informationssäkerhet.

Enligt revisorernas skrivelse visar granskningen att det finns områden som går att utveckla och listar ett antal utvecklingsområden i skrivelsen.

Revisorerna önskar att kommunstyrelsen yttrar sig kring granskningsrapporten i maj 2017 inför beslut i kommunfullmäktige i juni 2017.

Handlingar i ärendet:
De förtroendevalda revisorernas skrivelse 13 februari 2017 med bilagd granskningsrapport från PwC om Granskning av IT-verksamheten och arbetet med informationssäkerhet i Västerviks kommun

Kommunfullmäktige
593 80 Västervik
0490-25 40 00 (tfn)
0490-25 40 61 (fax)
www.vastervik.se
kommunfullmaktige@vastervik.se

KOMMUNENS REVISORER

2017-02-13

Kommunfullmäktige
Kommunstyrelsen

Granskningsrapport gällande "IT-verksamheten och arbetet med informationssäkerhet i Västerviks kommun"

På uppdrag av de förtroendevalda revisorerna i Västerviks kommun har PwC AB genomfört denna granskning.

Syftet med granskningen är att klargöra vilka eventuella områden som kommunen behöver utveckla för att uppnå en optimal IT-leverans i alla delar inklusive IT- och Informationssäkerhet.

Granskningen visar att så **bara delvis** är fallet och förbättringar bör göras.

Vi revisorer vill, med granskningen som grund, poängtera följande utvecklingsområden:

Kommunen bör säkerställa en tydlig samordning på strategisk nivå avseende IT-förvaltning och utveckling, samt för att driva den digitala agendan för kommunen.

Kommunen bör tillsätta en särskild ansvarig på övergripande nivå med ansvar att samordna samtliga frågor rörande e-tjänster och digitalisering.

Kommunen behöver än mer tydliggöra och kommunicera den beslutade strategin, ambitionsnivån och planen för vilka e-tjänster som ska erbjudas.

Kommunen bör komplettera de styrande dokumenten med en övergripande IT-strategi/e-strategi.

Kommunen bör överväga att införa kvalitetsmått för infrastruktur och kommun-gemensamma system.

IT-avdelningen bör införa en strukturerad jourverksamhet.

Kommunen bör skapa en plan för startegisk kompetensörsörjning inom IT.

Kommunen bör säkerställa att rollen som informationssäkerhetsansvarig får tillräckligt med tid och mandat.

VMEAB:s arbete med informationssäkerhet och teknisk säkerhet bör kunna bidra med inspiration till övriga delar av kommunen.

Västerviks kommun bör snarast tillsätta en ansvarig för PUL och den kommande dataskyddsförordningen.

För att undvika att känslig information blir tillgänglig för obehöriga bör kommunen säkerställa att det finns tydliga rollbeskrivningar för varje tjänst, samt vilka behörigheter dessa roller har knutna till sig.

Revisorerna önskar svar från Kommunstyrelsen senast 2017-05-22.

För kommunens revisorer

Britt-Louise Källmark
Ordförande

Saad Benatallah
Vice ordörande

Bilaga: granskningsrapport

www.pwc.se

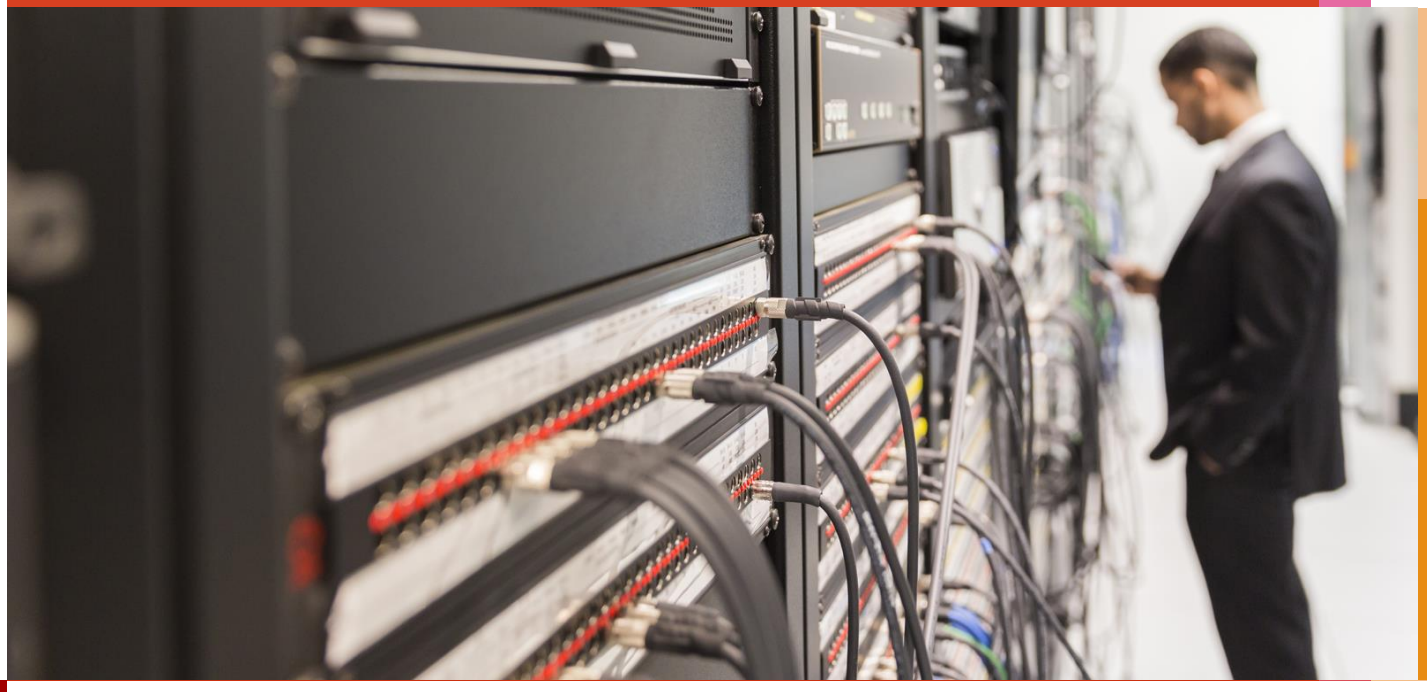
Västerviks kommun

Granskning av IT verksamheten och arbetet med informationssäkerhet i Västerviks kommun

November 2016

Västerviks Kommun

Februari 2017



pwc

Innehåll

Sammanfattning

1 Optimal IT-leverans

- Vår övergripande bedömning är att IT-verksamheten till viss del uppfyller revisionsfrågans innebörd. Det finns en medvetenhet om vad som krävs för att närma sig en optimal IT-leverans. Den främsta observationen är behovet av en tydligare samordning på övergripande och strategisk nivå för att säkerställa en effektiv IT-leverans och för att skapa förutsättning för att hela kommunkoncernen ska kunna dra nytta av digitaliseringens möjligheter.
- Det finns utvecklingspotential inom ett flertal områden såsom; övergripande strategisk IT-styrning och samordning, processorientering och kvalitetssäkring av IT inom IT-avdelningen såväl som i verksamheten.
- Granskningen visar att kommunen har genomfört delar av rekommendationerna i den övergripande IT-granskningen 2013. Rekommendationerna är dock inte helt slutförda. Exempel på slutförda åtgärder är framtagande av en katastrofplan för IT och etablering av en gemensam projektmodell för kommunen.

2 Teknisk IT-säkerhet

- Denna del av rapporten är sekretessbelagd i enlighet med enligt 18 kap. 8§ offentlighets- och sekretesslagen (2009:400).

3 Ändamålsenlig informationssäkerhet

- Området informationssäkerhet behöver utvecklas och stärkas inom hela kommunkoncernen. Det behövs även ett tydligare strategiskt arbete som innefattar hela kommunkoncernen.
- Kommunen behöver tydliggöra målbild och definiera ambitionsnivån på ett tydligt och konkret sätt.
- Kommunen behöver ta ett helhetsgrepp kring frågan hur man ska förbereda kommunkoncernen för det kommande dataskyddsdirektivet vilket ställer högre krav på personuppgiftshantering.
- Kommunens anställda bör utbildas och fortbildas kontinuerligt inom informationssäkerhetsområdet för att höja lägstanivån samt för att uppnå god praxis.
- Det är positivt att kommunkoncernen genomfört en satsning inom informationssäkerhetsområdet, samt har etablerat en tjänst som informationssäkerhetssamordnare. Det är viktigt att rollen får det mandat och stöd från kommunstyrelsen som krävs för att lyckas med sitt uppdrag.

Inledning

Granskningen som har genomförts av Västerviks kommuns IT-verksamhet* och arbete med informationssäkerhet har varit omfattande. Resultatet visar att det finns ett flertal områden som kommunen i varierande omfattning behöver ta hänsyn till och arbeta vidare med.

- Vår generella bedömning, vilken vi också vill lyfta fram, är att kommunen på övergripande nivå under de senaste åren har arbetat proaktivt inom ett flertal områden och där tagit ett antal viktiga steg för att utveckla sin IT-verksamhet mot större medborgarnytta, en bättre intern effektivitet, samt öka kunskapen och beredskapen inom informationssäkerhetsområdet. Vi uppfattar att det finns en ambition och vilja att utvecklas mot en modern kommun med stöd av bland annat digitala lösningar.
    - Samarbetet inom Cesam Öst är ett tydligt exempel som visar på att kommunen har ambitionen att vara i framkant gällande digitalisering och att möta kommande förväntningar på smarta digitala lösningar. Med detta samarbete visar också kommunen att man tänker utanför ramarna och söker samarbeten med god potential, för att sedan kunna bli en förebild för t ex den egna regionen.
    - Etableringen av den relativt nya funktionen som informationssäkerhetssamordnare åskådliggör att kommunen prioriterar och ser vikten av ett ökat fokus på informationssäkerhetsområdet och dess specifika utmaningar.
- För att fortsätta utvecklas behöver Västerviks kommun stärka den övergripande styrningen och samordningen av IT-verksamheten på strategisk nivå. Detta kan ske genom en tydligt utpekad funktion eller roll, som på övergripande nivå äger samordningsansvaret på ledningens uppdrag. Vidare bör inriktningen kommuniceras till verksamheten på ett mer organiserat sätt för att säkerställa att verksamheten drar åt samma håll både på kort och lång sikt, t ex inom ramen för arbetet med vision 2030.
- Granskningen visar att det framför allt inom IT- och informationssäkerhetsområdet finns ett antal kritiska områden där kommunen skyndsamt bör genomföra åtgärder. En del av dessa åtgärder är av relativ enkel art, som efter genomförande kommer att innebära att kommunens IT-verksamhet är bättre rustad och därmed ha en god och säker grund för det fortsatta utvecklingsarbetet.
- De rekommendationer som vi bedömer är mest prioriterade är sammanfattade på följande två sidor.

**Med IT-verksamhet avses alla IT-relaterade funktioner och IT-relaterat arbete inom kommunkoncernen, inklusive förvaltningar och bolag.*

Prioriterade rekommendationer

Optimal IT-leverans

Följande rekommendationer utgör vår sammanfattande prioritering inom området optimal IT-leverans.

1. Kommunen bör säkerställa en tydlig samordning på strategisk nivå avseende IT-förvaltning och utveckling, samt för att driva den digitala agendan för kommunen.
2. Kommunen bör tillsätta en roll på övergripande nivå med ansvar att samordna samtliga frågor rörande e-tjänster och digitalisering. Rollen bör ha ansvaret för att fånga upp verksamhetens behov och prioritera dessa i förhållande till kommunens strategi, utveckling och vision.
3. För att lyckas över tid behöver kommunen än mer tydliggöra och kommunicera den beslutade strategin, ambitionsnivån och planen för vilka e-tjänster som ska erbjudas, samt dra nytta av den effekthemtagningsmodell som finns inom Cesam Öst. Den ambitionsnivå som kommunen väljer avseende e-tjänster bör vara en viktig komponent i arbetet med vision 2030.
4. Kommunen bör komplettera de styrande dokumenten med en övergripande IT-strategi/e-strategi inklusive tillhörande handlingsplan samt säkerställa att dessa är kommunicerade i hela verksamheten.
5. Kommunen bör överväga att införa kvalitetsmått i form av SLA för infrastruktur och kommungemensamma system. IT-avdelningen bör också införa en strukturerad jourverksamhet som innebär att felanmälan för kritiska system kan ske och åtgärdas inom en överenskommen tid även utanför normal kontorstid. Detta kommer att skapa en tryggare situation för verksamheten, samt avlasta enskilda personer inom IT som i dagsläget bedriver jour ad hoc.
6. Kommunen bör fortsätta arbetet med processorientering av IT-verksamheten. Ta stöd i etablerade ramverk såsom ITIL för IT-avdelningen, samt förvaltningsmodellen Pm3 som skapar goda förutsättningar för en effektiv systemförvaltning i verksamheten.
7. Kommunen bör skapa en plan för strategisk kompetensförsörjning inom IT för att säkerställa att man får tillgång till rätt kompetens över tid.
8. Kommunen bör införa en modell/struktur för nyttorealiseringar för att säkerställa att gjorda investeringar får förväntat utfall.

Forts. Prioriterade rekommendationer

Teknisk IT-säkerhet och Ändamålsenlig informationssäkerhet

Följande rekommendationer utgör vår sammanfattande prioritering inom områdena IT-säkerhet och Ändamålsenlig informationssäkerhet.

1. Kommunen bör fortsätta att utveckla och stärka informationssäkerhetsarbetet inom hela kommunkoncernen. Västerviks kommun har sedan våren 2016 en informationssäkerhetssamordnare som har det övergripande samordningsansvaret för informationssäkerheten. Vi bedömer detta vara ett bra första steg och en riktad satsning i arbetet med att utveckla informationssäkerheten inom kommunen. Det är viktigt att säkerställa att rollen får tillräckligt mandat för att kunna genomföra viktiga förändringar.
2. Det behövs ett krafttag för att höja nivån på den tekniska IT-säkerheten, b la genom att införa en roll som har det övergripande tekniska ansvaret för säkerhetsarbetet inom IT-organisationen.
3. Det grundarbete inom informationssäkerhet som gjordes 2011-2013 behöver uppdateras och implementeras i större grad inom kommunkoncernen. Ett särskilt fokus bör ligga på de förvaltningar som hanterar känslig information såsom personuppgifter, vilka kommer ha ett mer omfattande arbete med att anpassa sig till den nya dataskyddsförordningen som träder i kraft under 2018. Det kommunala bolaget VMEAB, som är i framkant i sitt arbete med informationssäkerhet och teknisk säkerhet, skulle med fördel kunna bidra med inspiration till övriga delar av kommunen.
4. Västerviks kommunkoncern bör snarast tillsätta en ansvarig roll för PUL och den nya dataskyddsförordningen. Vidare bör kommunen starta upp ett formellt projekt för att förbereda organisationen för den nya dataskyddsförordningen som träder i kraft 2018.
5. Kommunen bör säkerställa att det finns tydliga rollbeskrivningar för varje tjänst, samt information kring vilka behörigheter dessa roller har knutna till sig. Detta för att klargöra vilken information en roll bör ha tillgång till, och på så vis undvika att känslig information blir tillgänglig för obehöriga personer.

Bakgrund och syfte

Inledning

Revisorerna i Västerviks kommun har gett PwC i uppdrag att genomföra en granskning av IT verksamheten och arbetet med informationssäkerhet i Västerviks kommun.

Resultatet av granskningen presenteras i denna rapport.

Bakgrund

Kommunens revisorer har efter en genomförd risk- och väsentlighetsanalys beslutat att granska IT verksamheten och arbetet med informationssäkerhet i Västerviks kommunkoncern utifrån ett antal definierade revisionsfrågor. Med IT-verksamheten menas all IT-relaterad verksamhet inom kommunen, inklusive förvaltningarna och bolagen.

Om kommunen inte hanterar IT säkerheten på rätt sätt finns det risk att känslig information hamnar i orätta händer. Ett felaktigt hanterande av säkerheten kan leda till att kommunens trovärdighet ifrågasätts och detta kan även leda till förluster både vad gäller ekonomi och anseende.

Syftet med granskningen är att klargöra vilka eventuella områden som kommunen behöver utveckla för att uppnå en optimal IT-leverans i alla delar inklusive IT- och Informationssäkerhet.

Övergripande revisionsfrågor och delområden för granskningen

Inom ramen för granskningen har följande tre granskningsområden med var för sig formulerade övergripande och kompletterande revisionsfrågor definierats.

Revisionsområden - delområden

- Optimal IT-leverans
- Teknisk IT-säkerhet
- Ändamålsenlig Informationssäkerhet

Övergripande Revisionsfrågor

1 Optimal IT-leverans

- Är användningen av resurser organiserad, strukturerad och kontrollerad för att ge och matcha en optimal IT-leverans, och ett optimalt verksamhetsstöd för hela kommunen inklusive bolagen?
- Vilka rekommendationer från den övergripande IT-granskningen 2013 har genomförts?

2 Teknisk IT-säkerhet

- Är Västerviks kommunkoncerns nuvarande IT-säkerhet tillräcklig för att minimera risker för obehörigt intrång av interna och externa aktörer?
- Uppfyller Västerviks kommunkoncern kraven för vad som anses som god praxis gällande teknisk IT-säkerhet?

Syftet med denna del av granskningen är att identifiera sårbarheter i Västerviks kommuns förvaltningar och bolags interna nätverk genom tekniska tester.

3 Ändamålsenlig informationssäkerhet

- Arbetar kommunens bolag och förvaltningar systematiskt med sitt informationssäkerhetsarbete?
- Finns det tydliga processer inom kommunkoncernen för informationssäkerhet med avseende på:
  - Organisation
  - Styrning, ledning och uppföljning
  - Utbildning
  - Kompetens

Syftet med denna del är att bedöma om informationssäkerhetsarbetet i Västerviks kommunkoncern sker utifrån en ändamålsenlig styrning, uppföljning och kontroll.

Revisionsfrågor - delområden

1 Optimal IT-leverans

1. Är användandet av kommunens e-tjänster optimerat och uppfyller det den önskade servicenivå som man vill erbjuda?
2. Har Västerviks kommun inklusive bolagen organiserat sin IT-verksamhet i enlighet med god praxis för IT-styrning, förvaltningsstyrning och IT-drift?
3. Finns roller och ansvar tydligt definierade för att säkerställa en effektiv leverans av IT?
4. Är processen för framtagande av IT-budget och uppföljning av den dokumenterad och strukturerad?
5. Förekommer löpande uppföljning av kostnader och nyttorealisering för leverans av IT-stödet?
6. Finns någon form av innovationsråd eller motsvarande för att utveckla digitala tjänster till medborgarnas nytta?
7. Finns det ett långsiktigt arbete för att säkerställa att nyckelkunskaper knutna till IT finns tillgängliga för organisationen på medellång och lång sikt?

2 Teknisk IT-säkerhet

1. Vilken är skyddsnivån kopplat till rutiner, processer, back-up och bemanningen för att hantera ett intrångsförsök, systemhaveri eller liknande IT-incidenter?
2. Finns erforderliga styrdokument på plats för att reglera situationen vid en eventuell IT-incident, t ex:
   - Dokumenterade rutiner och processer?
   - Krisplan/Katastrofplan/Kontinuitetsplan /Disaster Recovery Plan (DRP) utformat för IT-incidenter?
   - Beslutskedjor, eskaleringsrutiner och ansvarsfördelning vid IT-incidenter?
3. Finns det ett systematiskt arbete för att upptäcka och motarbeta nya och framtida hotbilder kopplade till IT-miljön?

3 Ändamålsenlig informationssäkerhet

1. Hur ser arbetet med kontrollsystem, så som t ex behörighetstilldelning, ut inom kommunen?
2. Finns det en tydlig målbild och definierad ambitionsnivå för arbetet med informationssäkerhet för samtliga avdelningar av kommunkoncernen?
3. Utbildas och informeras medarbetarna inom kommunen i frågor om informationssäkerhet?
4. Finns det en uttalad plan och tydlig styrning för arbetet med att anpassa kommunen till det kommande dataskyddsdirektivet som ställer ökade krav på informationssäkerhet och hantering av känslig data?
5. Finns rutiner kring olika roller och deras åtkomst till information och känslig information?
6. Har kommunen en kris eller katastrofplan för att skydda och bibehålla integriteten hos information eller känslig data vid en incident eller kris?

Metod

Metod

PwC har baserat granskningen på följande arbetssätt och metodik.

- Intervjuer med identifierade nyckelpersoner i kommunen, (se intervjulista, bilaga 1) samt inläsning och genomgång av tillgänglig dokumentation och styrande dokument.
- Granskningen baseras på beprövad metodik inom PwC.
  - I del 1 av granskningen har PwC:s metod ITM (IT Maturity analysis) använts. Metoden bygger på fem områden som tillsammans representerar IT-verksamheten inom en organisation. Metoden tar även hänsyn till så kallad ”good practice” inom IT generellt och jämför erhållet resultat med hur IT hanteras hos andra organisationer.
  - I del 2 och del 3 av granskningen har etablerade metoder för IT- och informationssäkerhet i form av penetrationstester och ett internationellt etablerat ramverk för Informationssäkerhet från NIST* (National Institute of Standards and Technology) tillämpats. NIST-ramverket bygger på att mognadsgrad och ändamålsenlighet avseende informationssäkerhet i en organisation analyseras på ett strukturerat sätt.

Avgränsning

- Erhållet material har granskats på en övergripande nivå.
- PwC har endast granskat den information som tillgängliggjorts för oss.

Optimal IT-leverans

Generella observationer

Följande observationer är av övergripande art och inte direkt kopplade till en specifik revisionsfråga. Däremot är de viktiga för den övergripande förståelsen.

- I samband med granskningen framkom att kommunen haft ett större problem med studenternas datorer på gymnasiet. Det som framför allt varit utmaningen är att problemet inte gått att isolera på ett tydligt sätt. Felet förefaller ha berott på att flertal mindre fel som påverkat varandra. Baserat på hur problemet har beskrivits för oss förefaller det finnas behov av att tydliggöra förändrings- och införandeprocesserna inom IT, samt att förenkla installationen på studenternas datorer.
- I intervjuerna med företrädare för kommunens ledning, både den politiska och den administrativa, framkommer att kommunen har en vilja att vara i framkant avseende digitala tjänster och funktioner. Det som dock lyfts är att det är svårt att införa ett digitalt arbetssätt i nämnder och ledningar inom kommunen. Ett flertal initiativ, såsom digitala handlingar till nämndmöten, har stoppats. Även inom kommunstyrelsen har det funnits ett motstånd för denna förändring. Ett digitalt arbetssätt behöver inte exkludera all pappershantering, det är viktigt att tänka på att ett förändringsarbete kommer att ta tid och kräva stort engagemang och uthållighet. Om kommunen har ambitionen att finnas i framkant, krävs dock att ledningen visar engagemang och vilja att förändra.
- Baserat på de rekommendationer som gavs i den tidigare rapporten, 2013, har kommunen arbetat med del förbättringsåtgärder;
  - En projektmodell för hela kommunen har tagits fram. Den förefaller vara känd, men ännu inte fullt ut implementerad. Det är viktigt att kommunen tydligt kommunicerar modellen och anger att den ska tillämpas, t ex för alla projekt över en viss budgetmässig och/eller omfattningsmässig tröskelnivå. Vidare bör användningen följas upp, inte minst för att kunna göra förbättringsåtgärder.
  - Det finns inget projektkontor eller motsvarande etablerat. Det finns inte heller något samordnat stöd för processer eller metoder. Kommunen bör överväga att införa detta för att underlätta användning av etablerade modeller och processer.
- Det saknas en tydlig uppdragsbeskrivning för IT-organisationen. Konsekvensen av detta är att det blir otydligt vad förvaltningarna och bolagen kan förvänta sig av IT-verksamheten, samt vad det egna ansvaret innefattar. I NKI-undersökningen från 2015 framkommer kritik mot IT-avdelningen kring delar som IT-avdelningen inte anser sig ha ansvar för. Detta är ett exempel på behovet av att tydliggöra de olika intressent-ernas uppdrag, samt att kommunicera ansvaret till hela organisationen.

Revisionell bedömning

Övergripande revisionsfrågor

" Är användningen av resurser organiserad, strukturerad och kontrollerad för att ge och matcha en optimal IT-leverans, och ett optimalt verksamhetsstöd för hela kommunen inklusive bolagen?"

"Vilka rekommendationer från den övergripande IT-granskningen 2013 har genomförts?

Bedömning

- Vår övergripande bedömning är att IT-verksamheten* till viss del uppfyller revisionsfrågans innebörd. Det finns en medvetenhet om vad som krävs för att närma sig en optimal IT-leverans. Den främsta observationen är behovet av en tydligare samordning på övergripande och strategisk nivå för att säkerställa en effektiv IT-leverans och för att skapa förutsättning för att hela kommunkoncernen ska kunna dra nytta av digitaliseringens möjligheter.
- Det finns utvecklingspotential inom ett flertal områden såsom; övergripande strategisk IT-styrning och samordning, processorientering och kvalitetssäkring av IT inom kommunen. En tydlig uppdragsbeskrivning för IT-organisationen bör tas fram. Vidare bör det påbörjade arbetet med tydliggörande av roller fortsätta för att uppnå en större effektivitet i IT-verksamheten.
- Granskningen visar att kommunen har genomfört delar av rekommendationerna i den övergripande IT-granskningen 2013. Flertalet av rekommendationerna är dock inte slutförda. Till exempel har arbete med uppdatering av styrande dokument och tydliggörande av system-ägarrollen påbörjats. Exempel på slutförda åtgärder är framtagande av en katastrofplan för IT och etablering av en gemensam projektmodell för kommunen. Avseende rekommendationen att inom ramen för e-strategin inkludera medborgarperspektivet, har kommunen efterfrågat vilka e-tjänster som önskas via lokaltidningen och på hemsidan.

**Med IT-verksamhet avses alla IT-relaterade funktioner och IT-relaterat arbete inom kommunkoncernen, inklusive förvaltningar och bolag.*

Revisionsfråga 1

Är användandet av kommunens e-tjänster optimerade och uppfyller de den önskade servicenivå som man vill erbjuda?

Observationer

- Granskningen från 2013 visade att Västervik saknade fastställda mål och ambitionsnivåer gällande IT-verksamheten i förhållande till mätning av samhälls- och medborgarnytta. Denna granskning visar att den observationen i stort fortfarande gäller. Samarbetet inom Cesam Öst har dock förutsättningar att kunna påvisa efterfrågade effekter, bl a genom att det finns en modell för detta inom Cesam Öst. Eftersom det är relativt nytt finns inte tillräckligt underlag för att kunna göra en fullständig bedömning om kommunens e-tjänster är optimerade och uppfyller den önskade servicenivån.
- Kommunen har sedan en längre tid ett flertal e-tjänster. Dessa är lättillgängliga och tycks vara relevanta för användarna. Vissa av tjänsterna är av enklare form, t ex formulär som ska skrivas ut för att sedan kompletteras. Andra tjänster är mer anpassade för digital hantering.
- För att skapa förutsättningar för en snabbare och mer effektiv utveckling av e-tjänster påbörjade kommunen under 2013 ett samarbete med Cesam Öst som under 2015 resulterade i ett formellt samarbetsavtal. Den e-tjänstplattform som används inom Cesam Öst har upphandlats gemensamt mellan kommunerna. Motivet bakom samarbetet är att få tillgång till fler e-tjänster, men även den kompetens och erfarenhet som byggts upp inom Cesam Öst.
- Samarbetet beskrivs som positivt av de intervjuade och det upplevs som att det finns en god utvecklingspotential för utveckling av gemensamma tjänster. Den fortsatta utvecklingen av e-tjänster innefattar ett 30-tal tjänster för Västervik, inklusive en utvecklingsplan för 2017. Det lyfts fram att tjänsterna tas fram baserat på verksamheternas behov och med hänsyn till medborgarnytta och interna prioriteringar.
- Under försommaren 2016 lanserades ”Mina sidor” och de tre första e-tjänsterna från samarbetet inom Cesam Öst. I och med detta har även användningen av kommunens e-tjänster ökat. Nyttjandet av de tidigare e-tjänsterna har varit varierande beroende på tjänst.
- Ambitionen med Cesam Öst är ett bra exempel på hur en kommun kan hitta former för en digital utveckling. Det framkommer dock i granskningen att det saknas en övergripande och tydlig strategi för e-tjänsteinförande i kommunen.
- Kommunen har inte heller utfört några kartläggningar för att identifiera vilka eventuella effektiviseringar som införande av olika e-tjänster skulle kunna leda till, t ex förändrat arbetssätt. I intervjuerna framkommer dock att det finns en medvetenhet kring detta och att det är något som kommunen planerar att arbeta vidare med.
- Kommunens bolag har i varierande omfattning infört ett flertal digitala lösningar och en stor del av servicen gentemot kunderna sker digitalt.

Rekommendationer

- Det finns stor potential att utveckla e-tjänster inom kommunen, inte minst mot bakgrund av den digitalisering som sker i samhället i stort. Inom ramen för Cesam Öst kan och bör Västervik nyttja både samarbetet och övriga kommuners erfarenhet för att utveckla sin förmåga att skapa e-tjänster.
- För att lyckas över tid behöver kommunen än mer tydliggöra och kommunicera den beslutade strategin, ambitionsnivån och planen för vilka e-tjänster som ska erbjudas, samt dra nytta av den effekthemtagningsmodell som finns inom Cesam Öst.
- Den ambitionsnivå som kommunen väljer avseende e-tjänster bör vara en viktig komponent i arbetet med vision 2030.

Revisionsfråga 2

Har Västerviks kommun inklusive bolagen organiserat sin IT-verksamhet i enlighet med god praxis för IT-styrning, förvaltningsstyrning och IT-drift?

Observationer

- Granskningen visar att kommunen har en IT-organisation som till viss del kan anses vara organiserad enligt god praxis. Det finns dock förbättringspotential inom ett flertal områden, främst inom IT-styrningsområdet, men även avseende processer och rutiner.
- Kommunen har en gemensam IT-avdelning med ca 15 anställda som framför allt hanterar drift och förvaltning av kommungemensamma system och infrastruktur. IT-avdelningen leds av kommunens IT-chef som rapporterar till chefen för Kommunservice.
- Infrastruktur och kommungemensamma system bedrivs i egen regi och av egen personal. Konsulter anlitas vid behov. Förvaltningar och bolag ansvarar för sina respektive verksamhetssystem. Granskningen visar att den tekniska och funktionella plattformen är uppdaterad och i stort fungerar väl. Processorientering har till viss del införts inom IT-avdelningen. Överlag är verksamheten nöjd med IT-leveransen. IT-avdelningen upplevs även stötta verksamheten på ett bra sätt i olika utvecklings-initiativ.
- Det finns en samordningsgrupp (IT-nätverk), med representanter från samtliga förvaltningar och bolag. Gruppen träffas 4 ggr/år för att utbyta information. Respektive deltagare ansvarar för att föra informationen vidare till sin ledningsgrupp. Det framkommer att IT-nätverket tillför ett tydligt värde, framför allt på taktisk och operativ nivå. Däremot anser ett flertal att gruppen inte har ett tillräckligt pådrivande mandat för att arbeta med strategiska frågor.
- Det saknas en gemensam strategisk agenda för IT, vilket fått till följd att den strategiska samordningen är spretig. Det finns planer på att etablera en IT-strategigrupp som komplement till IT-nätverket (se även revisionsfråga 3).
- Det finns ytterligare två samordningsgrupper; Säkerhetsnätverk och InfoSäkGrupp (dessa behandlas under Del 2-3 i denna rapport).
- Det finns ingen etablerad jourverksamhet för hantering av problem utanför kontorstid. Problem som uppstår löses ad hoc.
- Det finns inga garanterade kvalitetsparametrar för IT (SLA) definierade mot verksamheten. Frågan har diskuterats, men ännu inte lett till ett konkret införande. Det finns en önskan om tydliga SLA, framför allt från bolagen, men även de verksamheter som har behov av stöd vid IT-incidenter utanför normal kontorstid.
- Etablerad förvaltningsstyrningsmodell saknas, dock finns utsedda roller för systemägare och systemförvaltare inom verksamheten.

Rekommendationer

- Kommunen bör överväga att införa kvalitetsmått i form av SLA för infrastruktur och kommungemensamma system. IT-avdelningen bör även införa en strukturerad jourverksamhet som innebär att felanmälan för kritiska system kan ske och åtgärdas inom en överenskommen tid även utanför normal kontorstid. Detta kommer att skapa en tryggare situation för verksamheten, samt avlasta enskilda personer inom IT som i dagsläget bedriver jour ad hoc.
- Fortsätt arbetet med processorientering av IT-verksamheten. Ta stöd i etablerade ramverk såsom ITIL för IT-avdelningen, samt förvaltningsmodellen Pm3 som skapar goda förutsättningar för en effektiv systemförvaltning i verksamheten.
- Den övergripande IT-styrningen behöver stärkas för att säkerställa en bra samordning och prioritering av IT-initiativ, (se även rekommendationerna under revisionsfråga 1).
- Besluta och realisera den tilltänkta IT-strategigruppen, samt tydliggör IT-nätverkets roll och ansvar för att skapa tydligt fokus för olika frågor avseende IT och digitalisering.

Revisionsfråga 3

Finns roller och ansvar tydligt definierade för att säkerställa en effektiv leverans av IT?

Observationer

- Granskningen visar att det inom IT-avdelningen finns roller definierade för de funktioner som omfattas av en normalt organiserad IT-avdelning. För att minska sårbarheten vid t ex frånvaro finns ett visst kompetens- och rollmässigt överlapp inom IT-avdelningen.
- Flertalet medarbetare inom IT-avdelningen har gått ITIL-utbildning för att kunna utveckla ett större processtänkande och därmed arbeta mindre reaktivt, vilket förefaller ha fungerat bra, med en större tydlighet mellan olika roller i organisationen.
- Inom förvaltningarna och bolagen finns utsedda systemägare och systemförvaltare. Det finns även utsedda IT-kontaktpersoner som bland annat deltar i IT-nätverket. Det framkommer i granskningen att kompetensnivån är varierande, samt att rollen som systemägare och systemförvaltare till viss del upplevs otydlig och att ansvar inte alltid är tydligt kommunicerat.
- Frågan om vilken roll och ansvar IT-avdelningen ska ha i olika IT-utvecklingsfrågor är inte tydliggjort, vilket innebär att IT i vissa fall blir involverade sent i processen. Exempelvis vid inköp av nya IT-system inom förvaltningarna.
- Kommunen saknar en etablerad strategisk roll med ansvar för samordning av IT- och digitaliseringsfrågor på en övergripande strategisk och taktisk nivå.
- Kommunen har infört en roll som informationssäkerhetsamordnare. Utöver IT-chefens övergripande ansvar finns det i dagsläget ingen utpekad roll som ansvarar för IT-säkerhet (se även Del 2 och 3).

Risk

- Avsaknad av en övergripande roll för strategisk samordning av IT och digitaliseringsfrågor kan innebära att kommunen inte når sina mål avseende digitalisering och införande av e-tjänster.
- Det finns en risk att systemutvecklingsbehov förbises om systemägarrollen och dess ansvar är otydligt.

Rekommendationer

- Västervik bör tillsätta en roll på övergripande nivå med ansvar för att samordna samtliga frågor rörande e-tjänster och digitalisering. Rollen bör ha ansvaret för att fånga upp verksamhetens behov och prioritera dessa i förhållande till kommunens strategi, utveckling och vision. Detta bör ske i samråd med de kommunala bolagens specifika behov avseende deras affärsdrivande verksamheter.
- Säkerställ att systemägare och systemförvaltare har lämplig utbildningsnivå och är informerade om sin roll och vilket ansvar den innebär.

Revisionsfråga 4

Är processen för framtagande av IT-budget och uppföljning av den dokumenterad och strukturerad?

Observationer

- Granskningen visar att processen för framtagande av IT-budget och uppföljning till viss del är dokumenterad och strukturerad.
- Det finns en modell för framtagande av IT-budget. IT-avdelningen ansvarar för centralt finansierat IT-stöd såsom infrastruktur, PC-arbetsplats m m. Respektive förvaltning/bolag ansvarar för budgetering av sina respektive verksamhetssystem och förvaltnings/bolagsspecifika IT-stöd.
- Samordning mellan IT och förvaltningarna och bolagen sker i samband med budgetprocessen. Granskningen kan dock inte påvisa att det finns en tydlig struktur och dokumentation kring budgetprocessen.
- IT-avdelningen administrerar leverantörsavtal såsom gällande hård-vara, tillbehör och enstaka programvaror t ex MSOffice. Förvaltningarna med respektive systemägare administrerar sina verksamhetssystem. Avtalen sluts av upphandlingsenheten.
- Det finns en modell för finansiering av PC-arbetsplats, gemensamma IT-system och accesspunkter för trådlöst nät. Vidare handhar IT beställningar av leverantörsavtal (se ovan punkt). I vissa fall går leverantörsfakturan direkt till slutkund, i andra fall går leverantörs-fakturan till IT som sedan fakturerar vidare. I det senare fallet handlar det om större beställningar till olika verksamheter
- Förvaltningarna finansierar de funktioner de vill införa i system och applikationer. Inköp går via IT som hanterar bl a faktureringen gentemot leverantören. Det finns planer på att ändra detta, så att fakturorna går direkt till förvaltningarna
- Det framkommer viss osäkerhet kring kostnaden av IT och hur den förhåller sig till jämförbara verksamheter.

Rekommendationer

- För att uppnå större transparens avseende IT-kostnader gentemot förvaltningarna och bolagen bör Västerviks kommun utveckla och komplettera budgetprocessen med en tydligare dokumentation och struktur.

Revisionsfråga 5

Förekommer löpande uppföljning av kostnader och nyttorealisering för leverans av IT-stödet?

Observationer

- IT-kostnaderna nycklas ut till verksamheten baserat på en etablerad kostnadsmodell för de delar som hanteras av IT-avdelningen. Det framkommer dock att det till viss del är svårt att förstå modellen och därmed uppstår en otydlighet om bl a kostnadsnivån.
- Det framkommer att det på generell nivå inte sker någon specifik nytto- eller effektuppföljning av genomförda IT-initiativ.
- IT-kostnaden har sänkts under åren som konsekvens av nya avtal eller andra effektiviserande åtgärder. Detta upplevs som positivt av verksamheten.
- Det framkommer att det inte finns en strukturerad uppföljning av IT-kostnaderna i samverkan med förvaltningarna. IT har kunnat sänka kostnaderna under åren och ekonomin är i balans, av den anledningen har inte frågan om uppföljning efterfrågats.
- Det framkommer i granskningen att framför allt bolagen efterfrågar en uppföljning och kostnadsjämförelse av IT.
- Kommunen hade en period av dålig ekonomi under början 2010-talet. Detta har satt sin prägel på ekonomistyrningen. Målsättningen är att varje investering ska bära sig eller ge tydlig effekt för t ex medarbetarna.

Rekommendationer

- Kommunen bör tydliggöra kostnadsmodellen för IT-leveransen och kommunicera tydligt vad olika tjänster och funktioner kostar, t ex genom en tjänstekatalog för verksamheten.
- Kommunen bör säkerställa att samtliga IT-kostnader i kommunen följs upp på övergripande nivå för att få en god överblick och skapa förutsättningar för att kunna jämföra sig med andra liknade verksamheter.
- Kommunen bör införa en modell/struktur för nyttorealiseringar för att säkerställa att gjorda investeringar får förväntat utfall.

Revisionsfråga 6

Finns någon form av innovationsråd eller motsvarande för att utveckla digitala tjänster till medborgarnas nytta?

Observationer

- Granskningen visar att det inte finns ett etablerat innovationsråd eller motsvarande. Det saknas en tydlig samordning på strategisk nivå avseende utveckling av digitala tjänster, samt erforderliga styrande dokument, såsom en uppdaterad IT-strategi (alt. e-strategi) på övergripande nivå. Däremot har t ex gymnasieskolan tagit fram en egen IT (IKT)-strategi.
- Det framkommer att det finns behov av att utveckla digitala tjänster inom kommunen och att dessa ska hanteras på en strategisk nivå med rätt beslutsmandat.
- Det finns ett antal e-tjänster etablerade, vissa av dem är dock relativt enkla, t ex i form av blanketter. Inom ramen för det nyligen etablerade samarbetet med Cesam Öst finns stora förväntningar på att kunna erbjuda fler och bättre e-tjänster.

Risk

- Brist på övergripande samordning kan leda till att utvecklingen av digitala tjänster avstannar och att medborgarnyttan inte uppnås.

Rekommendationer

- Västervik bör säkerställa en tydlig samordning på strategisk nivå avseende både IT-förvaltning och utveckling samt att driva den digitala agendan för kommunen.
- Samarbetet med Cesam Öst förefaller vara ett bra initiativ för att uppnå en bra utveckling av e-tjänster. Det är dock viktigt att kommunen på övergripande strategisk nivå gör en tydlig plan för hur införandet ska ske, vilka tjänster som prioriteras och kopplar detta till den övergripande strategin och visionen.
    - Förslagsvis kan ett uppdrag till kommunikationsavdelningen ges för att marknadsföra alla digitala tjänster till invånarna.
- Kommunen bör komplettera de styrande dokumenten med en övergripande IT-strategi/e-strategi inklusive tillhörande handlingsplan.

Revisionsfråga 7

Finns det ett långsiktigt arbete för att säkerställa att nyckelkunskaper knutna till IT finns tillgängliga för organisationen på medellång och lång sikt?

Observationer

- Granskningen visar att kommunens ambition är att rekrytera långsiktigt och skapa förutsättningar för goda karriärvägar för dem som de vill stanna kvar i kommunen. Det finns dock generella utmaningar (demografiska/geografiska) med att hitta kvalificerad personal.
- Det finns ett behov av att lyfta kompetensen bland befintlig personal, men det förefaller inte finnas en tydlig och uttalad långsiktig plan kring kompetensförsörjning, t ex avseende systemägare/förvaltare.
- Det framkommer att det finns ett nyckelpersonberoende. T ex har bolag inom kommunen tidigare haft en specifik kontaktperson på IT-avdelningen. När personen har slutat har detta medfört att kunskapen kring bolagets verksamhetssystem försvunnit.
- Det framkommer att det finns viss IT-kompetens inom bolagen som skulle kunna bidra till en förstärkt IT-kompetens på generell nivå inom kommunen och därmed minska risken för nyckelpersonsberoende.
    - Bostadsbolaget har ett långsiktigt arbete kring kompetensutveckling, dels då de säkerställer att det är flera som kan systemen, på så sätt minskar de sårbarheten inom organisationen, dels arbetar de strategiskt och knyter till sig kompetens.

Risk

- Ett stort nyckelpersonberoende innebär en risk för den långsiktiga kompetensförsörjningen.
- Avsaknad av en långsiktigt plan för kompetensförsörjning kan innebära att IT-verksamheten blir sårbar.

Rekommendationer

- Västervik bör kunna dra nytta av den IT-kompetens som till viss del finns inom bolagen för att både bredda kunskapen och för att minska nyckelpersonberoendet.
- Det behövs en långsiktig plan kring kompetensutveckling inom IT-verksamheten som helhet, kopplat till kommunens vision och övergripande strategi. Utifrån kommunens behov ska kompetens säkerställas. Genom att göra en kompetenskartläggning kan Västervik identifiera vilken kompetensutveckling som krävs både inom IT-avdelningen och för verksamhetens förvaltning av IT-system.
- Kommunen bör skapa en plan för strategisk kompetensförsörjning inom IT för att säkerställa att kommunen får tillgång till rätt kompetens över tid.

Teknisk IT-säkerhet

Denna del av rapporten är sekretessbelagd i enlighet med enligt 18 kap. 8§ offentlighets- och sekretesslagen (2009:400).

Ändamålsenlig informationssäkerhet

Vad innebär ändamålsenlig informationssäkerhet?

En god informationssäkerhet syftar till att säkra en effektiv informationsförsörjning och att undgå allvarlig fel som påverkar möjligheten att bedriva en ändamålsenlig verksamhet.

Arbete med informationssäkerhet innebär att vidta preventiva åtgärder för att undvika att information kan förvanskas eller för att förhindra informationsläckage. Informationssäkerhet handlar även om att säkerställa att man alltid har tillgång till den information organisationen behöver för sin dagliga verksamhet, även om kris eller katastrof föreligger.

Den nivå av informationssäkerhet man behöver är helt avhängig den riskaptit man har, samt vilken hotbild man står inför som organisation. En organisation som hanterar mycket känslig information, exempelvis i form av personuppgifter i kundregister, lönelistor eller liknande, kan behöva mer skydd än en organisation som inte hanterar och lagrar liknande information.

Generella observationer

Följande observationer är av övergripande art och inte direkt kopplade till en specifik revisionsfråga. Däremot är de viktiga för den övergripande förståelsen.

- Det finns en bra och mycket ambitiös övergripande vision kring att utveckla informationssäkerheten inom Västerviks kommunkoncernen. Det behövs dock ett tydligare ledarskap och bättre styrning från ledningsnivå rörande informationssäkerhetsarbetet inom kommunkoncernen för att säkerställa att arbete till fullo implementeras.
- Det finns ett utvecklat grundarbete kring informationssäkerhet sedan tidigare satsningar. Det arbetet har dock inte implementerats till fullo i kommunkoncernen. Det finns nivåskillnader i organisationen där bland annat det kommunägda bolaget VMEAB skiljer sig från resten av bolagen och den kommunala förvaltningen. Därför bör grundarbetet åter implementeras med ett särskilt fokus på de förvaltningar som hanterar känslig information såsom personuppgifter och som kommer att ha en större utmaning med att anpassa sig till den nya dataskyddsförordningen som träder i kraft i maj 2018. VMEAB, som ligger långt fram i sitt arbete med informationssäkerhet och teknisk säkerhet, skulle med fördel kunna användas som inspiration för resten av organisationen.
- Granskningen visar att det finns stora nivåskillnader mellan det kommunala bolaget VMEAB och övriga bolag och förvaltningen i Västerviks kommun gällande bland annat arbetet med informationssäkerhet. För att utjämna dessa skillnader bör kommunen utvärdera VMEAB:s arbete med informationssäkerhet och ledningssystem och se på vilket sätt det kan nyttjas av organisationen.

Revisionell bedömning

Övergripande revisionsfrågor

”Arbetar kommunens bolag och förvaltningar systematiskt med sitt informationssäkerhetsarbete?”

Finns det tydliga processer inom kommunkoncernen för informationssäkerhet med avseende på: Organisation, Styrning, ledning och uppföljning, Utbildning, Kompetens?

Bedömning

- Baserat på de observationer vi gjort i denna granskning så kan vi konstatera att kommunen i dagsläget inte arbetar systematiskt med området informationssäkerhet. Detta främst på grund av att det föreligger stora nivåskillnader i hur arbetet med informationssäkerhet bedrivs inom kommunkoncernen, samt att det tidigare har saknats en roll som har det övergripande ansvaret för satsningen.
- Området informationssäkerhet behöver utvecklas och stärkas inom hela kommunkoncernen. Västerviks kommun har sedan våren 2016 en informationssäkerhetssamordnare som har det övergripande samordningsansvar för informationssäkerheten. Detta anser vi vara en riktad satsning och ett bra första steg i arbetet med att utveckla informationssäkerheten inom kommunen.
- Det kommunalägda bolaget VMEAB ligger förhållandevis långt fram i sitt arbete med informationssäkerhet, bland annat genom att vara ISO-certifierade och de nyttjar avancerade lednings- och ärendehanteringssystem som stöd i sitt arbete. Vi rekommenderar kommunen att ta tillvara den kunskap och kompetens som redan finns inom kommunen i det fortsatta arbetet med att utveckla kompetenserna inom förvaltningarna, då detta är ett snabbt och kostnadseffektivt sätt att föra arbetet framåt. Det finns en ansats för att förbereda kommunen för den kommande data-skyddsförordningen men det saknas helhetsgrepp och struktur för att leda arbetet vidare.
- Granskningen har inte observerat några tydliga och dokumenterade processer för hur arbetet med informationssäkerhet fortskrider inom kommunen.
- Rollen som informationssäkerhetssamordnare är relativt nyinsatt och har inte haft tid att genomföra större förändringar. I dagsläget är rollen placerad under säkerhetsavdelningen. Kommunen bör dock överväga att placera rollen som informationssäkerhetssamordnare direkt under kommunledningen samt säkerställa att rollen har erforderliga befogenheter för att driva igenom beslut. I dagsläget finns det inga tydliga mål för att utbilda och fortbilda personal kring området informationssäkerhet. Vi har dock observerat att det finns ett planerat projekt för att höja medvetande- och kunskapsnivån hos kommunalanställda. *Fler detaljer finns att hitta under revisionsfråga 3*.
- Bedömningen är att den generella kompetensnivån avseende informationssäkerhet är låg inom kommunkoncernen, särskilt hos de medarbetare som inte har säkerhet som primärt fokusområde. Informationssäkerhetssamordnaren är kompetent inom sitt område. Det är dock viktigt att rollen får möjlighet att fortbilda sig för att bibehålla och utveckla kompetensnivån.

Revisionsfråga 1

Hur ser arbetet med kontrollsystem, så som t ex behörighetstilldelning, ut inom kommunen?

Observationer

- De IT-system som driftas av den centrala IT-avdelningen i kommunen använder i huvudsak AD:t som kontrollsystem för inloggning på datorerna och för filåtkomst för hemkataloger och gemensamma kataloger. Det finns vissa system som är AD-integrerade fullt ut, men även sådana som endast utnyttjar tjänsten för inloggning. Vidare finns system där all behörighetstilldelning sker via systemförvaltaren.
- Granskningen visar att det inte finns något strukturerat och enhetligt arbete med behörighetstilldelning inom kommun eller inom bolagen. Det finns inget centralt system, eller en ansvarig för hur systeminformation ska läggas till eller tas bort. Vidare visar granskningen att det inte sker någon aktivitet för att skapa en bättre AD-integrering och/eller för att skapa en mer enhetlig behörighetstilldelning för kommunkoncernen.
- Det finns en checklista som chefer ska använda vid avslutande av anställning. Granskningen visar dock att checklistan saknar information om hur behörigheter ska hanteras, t ex att samtliga berörda systemägare ska kontaktas. Det framkommer att tidigare anställdas behörigheter finns kvar i systemen långt efter avslutad anställning.
- Idag finns det ingen övergripande funktion som ansvarar för att säkerställa att alla systemförvaltare får den information som behövs för att kunna fullfölja sina uppgifter.
- Ansvaret för att ha kontroll på behörigheter och förändringar finns idag på systemförvaltare, vilket innebär att kunskapsnivåerna är skiftande.

Risk

- Avsaknad av en central funktion där systembehörigheter skapas, tas bort och/eller förändras innebär en förhöjd risk för att individer ska få felaktiga eller dubbla behörigheter.
- Vid brist på ett strukturerat arbete med behörighetstilldelning ökar risken för att individer ska få för höga rättigheter, eller att rättigheter inte tas bort. Risken är att individer får tillgång till känslig information vid exempelvis en förändrad eller avslutad anställning.
- En generell risk med att låta systemförvaltare ha ansvar för att förändra behörigheter, är att förändringarna endast sker i deras ”egna” system och att systemförändringar inte sker på ett kontrollerat sätt.

Rekommendationer

- Kommunen bör etablera rutiner för att kontrollera behörighetstilldelning, samt säkerställa att dessa är likadana för hela kommunkoncernen. IT-avdelningen bör vara den funktion som ytterst ansvarar för att skapa rättigheter efter ”least privilege-principen”.
- Kommunen bör utveckla den checklista som används vid avslutande av anställning. Det tillägg som bör göras är att information om avslutande av anställning ska gå ut till samtliga systemägare samt att rättigheter ska plockas bort. Det är viktigt att det finns en effektiv process för detta.
- Kommunen bör införa en central roll som är ansvarig för att säkerställa att samtliga systemägare och annan berörd personal är uppdaterad med information kring förändringar av behörigheter.

Revisionsfråga 2

Finns det en tydlig målbild och definierad ambitionsnivå för arbetet med informationssäkerhet för samtliga avdelningar av kommunkoncernen?

Observationer

- Det finns en målsättning för Västerviks kommun rörande arbetet med informationssäkerhet, denna är uttryckt i *Säkerhetspolicyn*. I januari 2013 antogs riktlinjer för säkerhetsarbetet och i detta dokument fastslås att ett aktivt arbete kring informationssäkerhet ska genomföras inom kommunkoncernen. Denna vision är dock inte enhetlig för hela kommunkoncernen och finns inte heller tydligt dokumenterad och reviderad. Granskningen visar att den information som finns rörande målbilder inte heller är spridd till medarbetarna inom kommunen.
- Genom tillsättandet av en roll som informationssäkerhetssamordnare har kommunen gjort en tydlig satsning på området informationssäkerhet. Granskningen visar också att det finns ett pågående arbete med att revidera befintlig dokumentation och att skapa dokumentation som i dagsläget saknas.
- I kommunens *informationssäkerhetsinstruktion för användare, v. 1,2* klargörs att uppföljningsarbete är en viktig del av arbetet med informationssäkerhet, s. 6 (22):

  Uppföljning är en viktig del i informationssäkerhetsarbetet och ska årligen bevaka:

  - *att beslutade åtgärder är genomförda*
  - *att policy, riktlinjer och instruktioner följs*
  - *att internkontroll är genomförd*
  - *att policyn, riktlinjerna, instruktionerna och säkerhetsplanerna revideras vid behov*
- Det finns sedan tidigare en bra och grundläggande dokumentation för informationssäkerhet. Det framkommer dock att mycket av arbetet med löpande uppdatering och revidering av dokumentationen släpar efter.

Risk

- Utan tydligt dokumenterad målsättning för arbetet med informationssäkerhet är det svårt att säkerställa att arbetet går åt rätt håll och följer de tidplaner som kommunen satt upp.
- Om inte målbilder är enhetliga och spridda till alla berörda delar av kommunkoncernen är det svårt att etablera en grundläggande säkerhetsnivå. Det blir även svårt att säkerställa att alla förvaltningar och bolag inom kommunkoncernen har en gemensam målbild.
- Om dokumentation inte uppdateras kontinuerligt riskerar dess funktion att gå till spillo.

Rekommendationer

- Det behövs en tydlig strategi och riktlinjer för att skapa en samsyn kring informationssäkerhetsarbetet inom Västerviks kommun. Ett särskilt fokus bör läggas på det kommunala bolaget VMEAB, som i många avseenden kommit längre i sitt informationssäkerhetsarbete än den kommunala verksamheten: det går att lära mycket av hur VMEAB arbetar med t ex sitt ledningssystem. För att säkerställa att samtliga håller samma nivå och arbetar utifrån samma riktlinjer och principer bör man arbeta övergripande i hela kommunkoncernen.
- Säkerställ att de resurser som arbetar med informationssäkerhet får tillräckligt med tid avsatt för att bl a ta fram den dokumentation som krävs för det praktiska arbetet med informationssäkerhet.
- Då det redan finns ett pågående arbete med att revidera och utveckla befintlig dokumentation är det viktigt att kommunen aktivt stöttar informationssäkerhetssamordnaren i arbetet. Det är viktigt att tjänsten omfattar heltid, så att denne har en möjlighet att slutföra arbetet inom rimlig tid.

Revisionsfråga 3

Utbildas och informeras medarbetarna inom kommunen i frågor om informationssäkerhet?

Observationer

- Granskningen visar att arbetet med utbildning och fortbildning avseende informationssäkerhet inte genomförs. De roller som arbetar aktivt med informationssäkerhet och som arbetar med frågan på en strategisk nivå tycks ha goda grundkunskaper. Kunskapsnivån är dock varierande hos de medarbetare som inte har säkerhet som primärt arbetsområde. Många medarbetare anser inte själva att de har de kunskaper som krävs och som de skulle vilja ha.
- Det finns användarmanualer/lathundar om informationssäkerhet, dessa finns tillgängliga för alla medarbetare på intranätet FirstClass. Det finns dock en bristande medvetenhet bland medarbetarna om att dessa finns.
- Granskningen visar att det i dagsläget inte finns ett strukturerat arbete med att aktivt höja medarbetarnas informationssäkerhetsförmåga.
- I informationssäkerhetsinstruktion ”Utveckling, förvaltning och drift. V. 1,1.” klargörs följande instruktioner. *Utbildning ur ett informationssäkerhetsperspektiv ska ske av anställda i de olika roller, som anges i kapitel 2 Organisation och ansvar. Närmaste chef är ansvarig för att säkerställa att medarbetarna får nödvändig informationssäkerhetsutbildning*. Granskningen visar att instruktioner idag inte alltid följs och att medarbetare själva inte är medvetna om att de bör utbildas inom informationssäkerhet.
- Det finns ingen officiell utbildningsplan för att säkerställa att utbildning och fortbildning inom informationssäkerhet sker. Kommunen har dock ett nytt projekt med verktyget Nano-learning (”djungle map”) som ska fungera som hjälpmedel vid utbildning och informationsspridning.

Risk

- Om inte kommunen lyckas sprida den kunskap som finns utstakad i visioner, och på ett effektivt sätt implementerar arbetet i organisationen, finns en risk att informationssäkerhetsarbetet blir en pappersprodukt. Detsamma gäller om rollen informationssäkerhetssamordnare inte får det ansvar och de medel som krävs för att kunna driva igenom nödvändiga förändringar för att uppnå målen i säkerhetspolicyn.

Rekommendationer

- Kommunledningen behöver ange tydliga målsättningar och en tidplan för kommunens informationssäkerhetsarbete. Detta inkluderar att ange tydliga riktlinjer för den nivå av kunskap som medarbetare som inte har säkerhet som primärt arbetsområde bör ha, samt en plan för hur utbildning av informationssäkerhet ska ske.
- De initiativ som redan finns, exempelvis arbetet med Nano-filmer, är ett bra sätt för kunskapsspridning och något kommunen bör fortsätta att arbeta med. Informationsfilmer är ett effektivt sätt att nå ut till stora delar av kommunens anställda.
- Kommunen bör prioritera arbetet med att ta fram en tydlig utbildningsplan rörande informationssäkerhet. Utbildningsplanen bör innehålla information om vilken kunskapsnivå en viss roll/tjänst kräver, vilken typ av kunskapshöjande aktiviteter som bör genomföras samt vem som ansvarar för att utbildning och fortbildning sker fortlöpande. I ett initialt skede bör detta ansvar ligga på informationssäkerhetssamordnaren, vilken utvecklar planen tillsammans med förvaltningschefer och andra berörda chefer.

Revisionsfråga 4

Finns det en uttalad plan och tydlig styrning för arbetet med att anpassa kommunen till det kommande dataskydds-direktivet som ställer ökade krav på informationssäkerhet och hantering av känslig data?

Observationer

- Granskningen visar att det inte finns något specifikt projekt eller initiativ från ledningen för att förbereda kommunen för det kommande dataskyddsdirektivet. De ledare som lyfter frågan är de som ansvarar för informationssäkerhet och säkerhetsfrågor inom sin egen avdelning och därför är direkt berörda.
- Under granskningen har vi observerat att det inte finns någon tydlig styrning ifrån ledningsnivå gällande hur man ska förbereda organisationen för dataskyddsdirektivet. Vi ser också att det i dagsläget saknas en samordnande funktion för PUL-frågor, som skulle vara en naturlig placering för arbetet med det kommande dataskyddsdirektivet.
- I dagsläget ligger ansvaret på den nyligen tillsatta informationssäkerhetssamordnaren, som i samarbete med informationssäkerhetsgruppen och de ledare som själva intresserar sig för frågan, leder arbetet med att förbereda organisationen.
- Inom informationssäkerhetsgruppen är frågan om hur man ska förbereda organisationen inför den nya förordningen rest och finns med som en prioriterad punkt på dagordningen. I nuläget har deltagarna i informationssäkerhetsgruppen i uppgift att se över vad deras egen förvaltning/avdelning behöver för resurser för att hantera förändringarna.
- Inom de kommunalägda bolagen hanteras ansvaret för denna fråga av det utnämnda personuppgiftsombudet eller ledningen.

Risk

- Det är mycket svårare att uppnå ett bra resultat så länge det inte finns ett formellt projekt för att implementera förändringarna. Avsaknad av specifikt utsedda ansvariga kan innebära att frågan inte prioriteras eller helt faller mellan stolarna.
- I och med den nya dataskyddsförordningen kommer högre krav att ställas på rollen som personuppgiftsansvarig då denne blir personligt ansvarig för hanteringen av bland annat personuppgifter. Om den nya dataskyddsförordningen inte följs, och personuppgifter eller annan känslig information inte hanteras i enlighet med den, kan organisationen behöva stå för viten på upp till 20 miljoner euro.

Rekommendationer

- Västerviks kommunkoncern bör snarast starta upp ett formellt projekt för att förbereda organisationen för den nya dataskyddsförordningen.
- Kommunen bör snarast tillsätta en ansvarig roll för att hantera PUL och den kommande dataskyddsförordningen.
- Det krävs en tydlig styrning ifrån kommunledningen för att säkerställa att organisationen uppfyller de riktlinjer kommunen satt upp rörande informationssäkerhet.
- Vid tillsättande av den nya rollen som personuppgiftsbiträde/personuppgiftsansvarig krävs en tydlig rollbeskrivning och mandat, samt erforderlig kompetens eftersom komplexiteten kommer att öka med det nya direktivet.

Revisionsfråga 5

Finns rutiner kring olika roller och deras åtkomst till information och känslig information?

Observationer

- Granskningen visar att det saknas tydliga roll- och arbetsbeskrivningar för de olika tjänsteområdena inom förvaltningen i kommunen. Dokumenterade roll- och arbetsbeskrivningar är en grundläggande förutsättning för att kunna avgöra vilken nivå av information en specifik roll behöver.
- Det finns inget strukturerat arbete med att kategorisera vilken information olika roller och befattningar inom kommunen skall och bör ha tillgång till.
- Inom bolagen i kommunkoncernen är arbetet med roller och deras rätt till information mer utvecklat. För t ex VMEAB finns befattningsbeskrivningar inlagda i det ledningssystem de använder sig av. Även de andra bolagen ligger längre fram i arbetet med roller, även om det finns otydligheter på ledningsnivå.

Risk

- Utan tydliga roll- och arbetsbeskrivningar blir det svårt att avgöra vem som bör ha tillgång till vilken information, samt vilken nivå av information en viss roll förutsätter. Om arbetet sker ad hoc ökar risken att för höga rättigheter delas ut och att tillgången till information blir beroende av den individ som begär rättigheterna istället för av vilken roll det är som begär ut informationen.

Rekommendationer

- Västerviks kommunkoncern bör säkerställa att det finns tydliga rollbeskrivningar för varje tjänst, samt information kring vilka behörigheter dessa roller har knutna till sig. Detta för att klargöra vilken information en roll bör ha tillgång till för att på så vis undvika att en del individer tillskansar sig behörigheter de inte har (eller ska ha) behov av för sitt dagliga arbete.
- Det behövs ett tydliggörande kring vilken roll/tjänst som har rätt till vilken information. Urvalsprincipen bör baseras på ”principle of least privilege” (PLP), d v s att en person/roll aldrig har rätt till mer information än vad som är nödvändigt för att kunna utföra sitt dagliga arbete. PLP följer ”best practise” inom informationssäkerhet för organisationer och är därför att rekommendera som urvalsprincip för rättighetstilldelning.
- Förvaltningarna inom Västerviks kommunkoncern skulle kunna dra nytta av det arbete som redan har gjorts hos de kommunalägda bolagen då de länge arbetat med roll- och tjänstebeskrivningar. Exempelvis har VMEAB enligt egen utsago dokumenterade rollbeskrivning för samtliga anställda inom bolaget, samt efter behov därtill kopplade roller (rollbeskrivningar).

Revisionsfråga 6

Har kommunen en kris- eller katastrofplan för att skydda och bibehålla integriteten hos information eller känslig data vid en incident eller kris?

Observationer

- Det finns i nuläget inget strukturerat arbete med att klassa och kategorisera information utefter dess känslighet och skyddsvärde, varken vid kris eller vid daglig verksamhet. Däremot ser vi att informationssäkerhetssamordnaren har påbörjat ett arbete, det är bra.
- Den dokumentation som finns i form utav kris- och katastrofplaner, innehåller inte riktlinjer för hur kommunen bör agera för att säkerställa att integriteten hos kommunens informationstillgångar bibehålls även vid kris.
- De kris- och katastrofplaner som finns är i hög grad baserade på de standardplaner som MSB skapar och distribuerar, och inte direkt utformade för den egna organisationen.
- Kommunen har inte en kris- eller katastrofplan som klargör vilka åtgärder som ska vidtas för att skydda och bibehålla integriteten hos information och/eller känslig data.

Risk

- Då informationstillgångar inte kartläggs och information inte klassas, är det svårt att sätta en adekvat skyddsnivå för informationen i fråga.
- Om riktlinjer för hur kommunen säkerställer integriteten hos information vid kris och katastrof saknas är det svårt att kräva efterlevnad. Det är också svårt för medarbetare att veta hur de bör agera samt vem som är ansvarig för att säkerställa att information behandlas på ett sådant vis att dess integritet är säkerställd även vid en kris. Frågan kommer då inte att få det fokus den kräver om det inte finns med som en prioriterad punkt vid kris och katastrof.

Rekommendationer

- Västerviks kommun behöver initiera ett arbete med att se över befintliga planer och dokumentation, för att säkerställa att de är direkt användbara vid en kris. I samband med denna uppdatering bör kommunen säkerställa att aspekten ”skydda och bibehålla integriteten hos informationen” finns med.
- Kommunen behöver se över den befintliga dokumentation som finns rörande informationssäkerhet och säkerställa att den är enhetlig och uppdaterad.

Bilagor

Bilaga 1. Teknisk IT-säkerhet (sekretessbelagd)
Bilaga 2. Intervjulista
Bilaga 3. Ordlista

Bilaga 2. Intervjulista delområde 1 – Optimal IT-leverans

Namn	Roll	Verksamhet
Anders Björlin	Kommundirektör	Kommunledning
Christer Lund	Administrativ chef	Enheten för kommunservice
Thomas Kronstål	Kommunalråd	Kommunstyrelsen
Lennart Nilsson	IT-chef	IT-avdelningen
Per Larsson	IT-tekniker	IT-avdelningen
Joakim Jansson	Räddnings- och säkerhetschef	Enheten för räddningstjänst och samhällsskydd
Fredrik Carlsson	Informationssäkerhetsamordnare	Enheten för räddningstjänst och samhällsskydd
Sven-Åke Lindberg	VD	Bostadsbolaget Västervik
Per Allert	VD	Västervik Miljö & Energi AB
Gunnar Bohman	VD	Västervik Resort AB
Magnus Bengtsson	Förvaltningschef	Barn-och utbildningsnämnden
Jörgen Olsson	Förvaltningschef	Socialförvaltningen
Elisabeth Olsson	Kanslichef	Kommunledningen
Ola Karlsson	Förvaltningschef	Miljö-och byggnad

Intervjulista delområde 3 - Informationssäkerhet

Namn	Roll	Verksamhet
Lennart Nilsson	IT-chef	IT-avdelningen
Birgitta Aldebert/Jenny Gustafsson/ Charlotta Chronèer	Nämndsekreterare/Intendent/IT pedagog	Barn-och utbildningsnämnden/Gymnasiet/Barn- och utbildningsförvaltningen
Joakim Jansson	Räddnings- och säkerhetschef	Enheten för räddningstjänst och samhällsskydd
Peter Wahlin	IT-tekniker	IT-avdelningen
Mariana Hugosson	IT-ansvarig	Miljö-och byggnad
Ola Karlsson	Förvaltningschef	Miljö-och byggnad
Fredrik Carlsson	Informationssäkerhetssamordnare	Enheten för räddningstjänst och samhällsskydd
Carina Magnusson	HR-chef	Kommunledningen
Pelle Svensson/Pär Hallinder	Förvaltare bostadsbolag/IT- ansvarig	Bostadsbolaget Västervik
Rickard Wester/Christoffer Schmidt	Kvalitets- och miljöansvarig/Kundservicechef	Västervik Miljö & Energi AB
Therese Eriksson/Pia Berg (telefonintervju)	IT-ekonom/Kvalitetssamordnare	Förvaltningsstaben på Socialförvaltningen
Elisabeth Olsson	Kanslichef	Kommunledningen

Bilaga 3. Ordlista

AD - Active Directory. Är en katalogtjänst ifrån Microsoft som innehåller information kring olika resurser i en domän, exempelvis vilka användare och datorer som finns.

AD - integrering. AD-integrering innebär att system ifrån andra tillverkare är integrerade i domänen och ADt, vilket möjliggör för användarinformation att förflyttas mellan olika system.

DRP - Disaster Recovery Plan. En DRP är de dokumenterade processer eller procedurer tänkta att skydda en organisations IT-infrastruktur vid händelse av en katastrof.

ITIL - Information Technology Infrastructure Library. ITIL är är en samling principer för hantering av IT-tjänster.

ITM - IT-Maturity Analysis. ITM är PwCs egna modell för att bedöma och utvärdera mognadsgrad hos IT-organisationen. Metoden bygger på fem områden som tillsammans representerar IT-verksamheten inom en organisation och som även hänsyn till så kallad ”good practice” inom IT.

NIST - National Institute of Standards and Technology. NIST är en organisation som drivs av de amerikanska handelsdepartementet, vilka har utvecklat en modell för hantering av informations-och cybersäkerhet. En NIST-assessment är en metod för att utvärdera Cyberförmågor och säkerhetsarbete hos organisationer.

PEN-test. Penetrationstest är et försök att penetrera system och infrastruktur för att påvisa svagheter i befintlig infrastruktur.

PHISHING-attack. Är ett angreppssätt som går ut på att via mejl tillskansa sig användares kontouppgifter eller att lura användare att följa länkar innehållande skadlig kod.

PLP - Principle of Least Privilege. Är best practise inom informationssäkerhet, och handlar om den princip man antänder sig av när man delar ut behörigheter. Praxis är att så låga behörigheter som möjligt skall delas ut.

PM3 - Är en förvaltnings- och portföljsstyrningsmodell för hantering av organisationer.

SLA - Service Level Agreement. SLA är ett leverantörs eller förvaltningsavtal som reglerar svarstider och åtgärdstider vid incident eller anomali.