Kf § 12

Revisionsrapport om uppföljande granskning av IT-verksamheten och informationssäkerhet i Västerviks kommun

Dnr 2017/67-007

Kommunens revisorer har i skrivelse 6 februari 2018 överlämnat en revisionsrapport om uppföljande granskning av IT-verksamheten och informationssäkerhet i Västerviks kommun.

PwC har på uppdrag av kommunens revisorer genomfört granskningen och redovisar granskningen och dess resultat på kommunfullmäktige 26 februari 2018. Syftet med granskingen är att bedöma hur långt kommunen har kommit med att åtgärda de brister som framkommit i granskningen under 2016.

Kommunens revisorer lämnar bedömning och rekommendationer till kommunstyrelsen i skrivelsen. Revisorerna framför även att de önskar att svar på revisionsrapporten i april 2018.

Britt-Louise Å Källmark, ordförande kommunens revisorer, redogör för revisorernas bedömning.

Niklas Ljung, PwC, informerar om granskningen och dess resultat.

Jon Sjölander (M) ställer fråga till Niklas Ljung, som besvarar frågan.

Lars-Inge Karlsson (KD) deltar i debatten.

Yrkande
Ordföranden yrkar att revisionsrapporten remitteras till kommunstyrelsen för beredning av svar till kommunfullmäktige i april 2018.
Ordföranden finner att kommunfullmäktige har bifallit yrkandet.

Kommunfullmäktige beslutar
att revisionsrapporten om uppföljande granskning av IT-verksamheten och informationssäkerhet i Västerviks kommun remitteras till kommunstyrelsen för beredning av svar till kommunfullmäktige i april 2018.

Handlingar i ärendet:
Kommunens revisorers skrivelse 6 februari 2018 med bilagd revisionsrapport från PwC daterad 13 december 2017

Expedieras till:
Kommunstyrelsen
Kommunens revisorer

2018-02-06

Till
Kommunfullmäktige

Granskning av IT-verksamheten och arbetet med informationssäkerhet i Västerviks kommun

PwC har på uppdrag av de förtroendevalda revisorerna genomfört en uppföljning av den granskning av kommunens IT-säkerhet som genomfördes under 2016. Syftet har varit att bedöma hur långt kommunen har kommit med att åtgärda de brister som framkommit i granskningen under 2016.

Den övergripande bedömningen är att IT-verksamheten ***till viss del*** uppfyller den övergripande revisionsfrågan. Det finns ett bra säkerhetstänkande och kommunen har upprättat en handlingsplan samt vidtagit en rad åtgärder för att uppfylla erhållna rekommendationer från 2016 års revision.

Västerviks kommun har efter revisionen som utfördes 2016 visat en tydlig ambition att uppfylla de rekommendationer som förmedlades vid den tidpunkten. Kommunen har genom detta visat en medvetenhet gällande vikten av god teknisk IT-säkerhet. Näst intill alla rekommendationer har tagits i beaktande och arbete för att fullfölja dem har påbörjats. Dock har vissa initiativ stannat av, främst på grund av tids- och resursbrist.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Ta fram en koncernövergripande IT-strategi samt strategi för IT-säkerhet.
- Göra en kraftsamling för att komma till rätta med avsaknaden av och bristen på nödvändiga IT-relaterade dokument så som rutiner, regelverk, instruktioner, policy och handböcker.
- Kommunen bör påskynda uppgraderingen av klienter med äldre Windows versioner till nyare operativsystem, samt omgående uppdatera serversystem som har utgången s.k. ”end-of-life” mjukvara.
- IT-miljön bör regelbundet skannas efter sårbarheter. Sårbarhetsskanning ger kommunen möjlighet att upptäcka sårbarheter och därmed agera innan interna och externa hot realiseras.
- Säkerställa att kommunikationskedjor och ansvarsförhållanden vid en händelse eller incident tydliggörs.

Vi förtoendevalda revisorer ställer oss bakom granskningens slutsatser och rekommendationer och överlämnar härmed granskningsrapporten.
Vi önskar svar på rapportens rekommendationer samt vilka åtgärder som man planerar att vidta senast den 15 april 2018.

För Västerviks kommuns revisorer

Britt-Louise Åberg Källmark
Ordförande

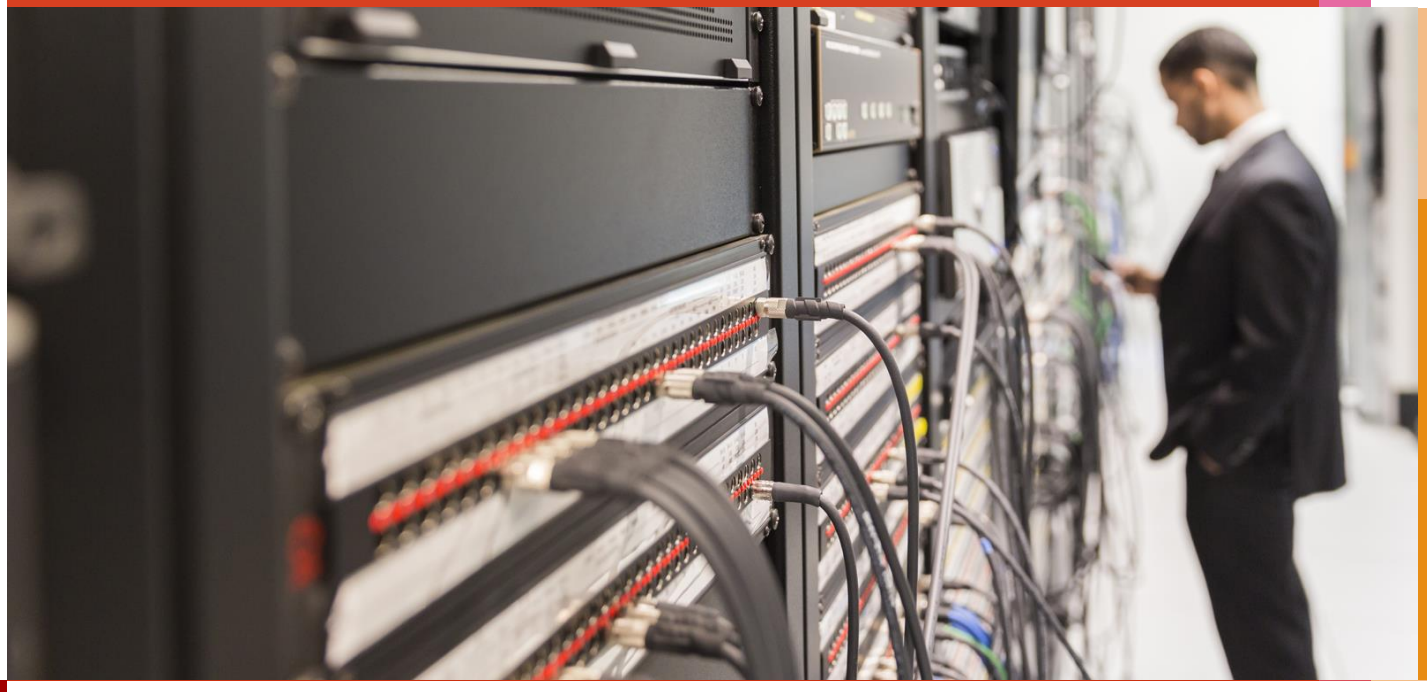
Bilaga: Granskningsrapport ……

www.pwc.com/se

Västerviks kommun

Granskning av IT-verksamheten och arbetet med informationssäkerhet i Västerviks kommun

December 2017



Niklas Ljung
Ida Ek

13 december 2017

Innehåll

Sammanfattning

PwC:s övergripande bedömning är att IT-verksamheten vid Västerviks kommun till viss del uppfyller den övergripande revisionsfrågan.

- Västerviks kommun har efter revisionen som utfördes 2016 visat en tydlig ambition att uppfylla de rekommendationer som förmedlades vid den tidpunkten. Kommunen har genom detta visat en medvetenhet gällande vikten av god teknisk IT-säkerhet. Näst intill alla rekommendationer har tagits i beaktande och arbete för att fullfölja dem har påbörjats. Dock har vissa initiativ stannat av, främst på grund av tids- och resursbrist.

- Kommunen behöver fortsätta att utveckla sin förmåga att förebygga och hantera IT-säkerhetsincidenter. Exempel på områden som behöver förbättras är beredskapen inom IT-organisationen, förmågan att hantera hot och sårbarheter i IT-miljön samt ansvarsfördelningen för IT-säkerhetsområdet.

- Kommunen bör ta ett krafttag för att komma tillrätta med den bristande tekniska dokumentationen. För att göra detta behövs avsättas tid och resurser utöver den ordinarie verksamheten.

- Det är positivt att IT-verksamheten har upprättat kontrollpunkter för IT-säkerhet samt eliminerat viss del av det ursprungliga personberoendet genom att tillse att det finns minst två personer med god insyn i kritiska funktioner inom IT-verksamheten.

Inledning

Revisorerna i Västerviks kommun har gett PwC i uppdrag att genomföra en uppföljning av den granskning av kommunens IT-säkerhet som genomfördes under 2016.

Resultatet av den uppföljande granskningen presenteras i denna rapport.

Bakgrund och syfte

Under hösten 2016 genomförde PwC en granskning av IT- och informationssäkerhetsområdet inom Västerviks kommun på uppdrag av kommunens revisorer.

Granskningen omfattade tre områden; *Optimal IT-leverans, Teknisk IT-säkerhet, samt Ändamålsenlig Informationssäkerhet*.

Syftet med denna uppföljande granskning är att få en samlad bild och status på de åtgärder som kommunen vidtagit, alternativt arbetar med, för att möta de brister som granskningen 2016 påvisade för **område 2, Teknisk IT-säkerhet**.

Följande granskningsfrågor för område 2 utvärderades 2016:

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

Övergripande revisionsfråga och kontrollfrågor för denna granskning

Revisionsfrågan och dess kontrollfrågor har sin grund i de rekommendationer gällande teknisk IT-säkerhet som förmedlades i samband med granskningen år 2016.

Revisionsfråga och kontrollfrågor

Har Västerviks kommuns aktivt arbetat för att uppfylla de rekommendationer gällande teknisk IT-säkerhet som förmedlades i samband med den revision som utfördes år 2016

Kontrollfråga 1	***Arbetar kommunen med IT-säkerhet på en nivå som anses tillräcklig för att förhindra interna och externa hot från att realiseras?***
Kontrollfråga 2	***Har Västervik kommun en tillräcklig beredskap för att hantera IT-incidenter?***
Kontrollfråga 3	***Finns erforderliga styrdokument och ansvarsfördelning gällande IT-säkerhet och incidenthantering?***

Metod

Granskningen har baserats på PwC:s metod ITM (IT Maturity analysis). 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. Rekommendationerna från den tidigare rapporten ligger till grund för fokusgraden inom respektive område.

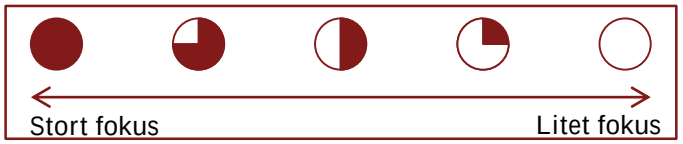
Informationssäkerhet
- Finns det en tydlig målbild och ansvarsfördelning, för arbetet med informationssäkerhet? Hur arbetar man med att klassificera och kategorisera data samt känslig data? Finns det ett arbete för att förbereda organisationen på omställningarna med nya dataskyddsförordnigen (GDPR)?

Teknisk säkerhet
- Hur arbetar organisationen med att utveckla och hålla sig á jour med den tekniska säkerheten? Hur säkerställer man säkerheten hos externa system? Hur kontrollerar och managerar man devices? Hur säkerställer man en fullgod säkerhet på laptops/plattor och mobiler. Är driftorganisationen ordentligt rustad att klara ett systemhaveri?

Drift och utveckling
- Drift: Hur ser den dagliga driften ut? Hur arbetar man aktivt med leverantörsstyrning? Hur ser processer, rutiner, dokumentation samt loggföring ut för driftorganisationen?
- Utveckling: Hur ser utvecklingsarbetet ut? Finns det tydliga, processer, rutiner och dokumentation som reglerar arbetet?

Organisation och personal
- Hur ser rollfördelningen ut inom organisationen? Finns det en tydlig ansvarsfördelning? Är bemanningen i driftorganisationen samt service-desk tillräcklig och har de rätt kompetens? Är organisationen strukturerad och uppbyggd för att inte hamna i beroende till nyckelpersoner?

Utveckling och framtid
- Hur arbetar organisationen med förändringsarbete, utveckling och målsättningar? Finns det planer och strategier för att leda organisationen framåt? Finns tydliga mål och visioner från ledningen uppsatta och dokumenterade?



Metod (forts.)

Insamling av data

Följande metodik har använts för att samla in data:

- Intervjuer med nyckelpersoner i kommunen, (se intervjulista, bilaga 1)
- Inläsning och genomgång av tillgänglig dokumentation och styrande dokument.

Avgränsning

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

Resultat

Generella observationer

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

- IT-chefen går i pension om sex månader och kommunen har ännu inte tillsatt någon ersättare. Tillsätts denna roll i god tid så ges den nya personen chansen att sätta sig in i verksamheten ordentligt innan tillträde. Det är viktigt att den nya personen får tillgång till så mycket som möjligt av den erfarenhet och kunskap som den nuvarande IT-chefen besitter.
- IT-kundtjänst är sårbara när det gäller frånvaro. I de fall då en av tre anställda vid IT-kundtjänst är frånvarande så uppstår problem då man inte hinner med att hantera inkommande ärenden effektivt.
- Vår bedömning är att det är en stor nackdel att IT-kundtjänst inte sitter tillsammans med resten av IT-avdelningen. Framför allt innebär det att det inte blir en naturlig kunskapsspridning mellan IT-tekniker och kundtjänst och vice versa.
- Med hänsyn till det stora IT-beroende som finns i dagens moderna samhälle är det viktigt att beslutsfattare i kommunstyrelse och ledning har en god insyn och förståelse för området som sådant, men också avseende de risker och hotbilder som detta innebär. Det framkommer i granskningen att IT-och informationssäkerhetsområdet har svårt att få gehör för sina behov då det uppfattas vara många steg mellan de som arbetar med detta och kommunstyrelsen/ledningen. Det finns en risk att när informationen ska passera många steg innan den når beslutsfattare, så har den en benägenhet att byta karaktär/förvanskas. Erfarenheten visar att i de fall dessa funktioner finns i direkt anslutning till beslutsfattare och kan direktrapportera i relevant omfattning så ökar sannolikheten att korrekt information når fram, vilket leder till effektiva och snabba beslut där så krävs.
- Arbetet med GDPR tar en stor del av informationssäkerhetssamordnarens tid. Detta har bland annat inneburit att den informationssäkerhetsgruppering som startades med anledning av föregående revision har avslutats på grund av tidsbrist.
- Kommunens personal utbildas inte inom IT- och informationssäkerhet. Den nano-utbildning som skulle utformas för ändamålet har eftersatts på grund av resursbrist samt kostnader. Vår bedömning är att det var ett bra initiativ som bör återupptas i någon form.
- Det finns inga etablerade kvalitetsmått i form av SLA:er mellan förvaltningar och IT.
- Många applikationer är fortfarande fristående från kommunens AD. Detta leder till att behörigheter i dessa hanteras i applikationen snarare än centralt i AD. Detta innebär en risk eftersom kontrollen av relevanta behörigheter försvåras.

Revisionell bedömning

Övergripande revisionsfråga

Har Västerviks kommuns aktivt arbetat för att uppfylla de rekommendationer gällande teknisk IT-säkerhet som förmedlades i samband med den revision som utfördes år 2016

Bedömning

- Vår övergripande bedömning är att IT-verksamheten ***till viss del*** uppfyller den övergripande revisionsfrågan. Det finns ett bra säkerhetstänkande och kommunen har upprättat en handlingsplan samt vidtagit en rad åtgärder för att uppfylla erhållna rekommendationer från 2016 års revision. Dessvärre har vissa av åtgärder inte kunnat genomföras fullt ut. Orsaken bakom detta har ofta varit brist på resurser i form av tid och pengar. Exempel på initiativ som har stannat av är informationssäkerhets-gruppen samt den nano-utbildning som skulle riktas mot användarna för att öka medvetandet gällande IT- och informationssäkerhet.
- Kommunen har minskat risken för personberoende genom att tillse att det finns minst två personer med god insyn i varje undergruppering inom IT-verksamheten. Utöver detta har man framförallt på undergrupperingen systemteknik tillsett att upprättad teknisk dokumentation är förståelig även för dem utan detaljerad insyn i deras rutiner. IT-infrastruktur har upprättat kontrollpunkter för centrala system i IT-miljön genom att implementera ett nytt system för loggning.
- Koncernövergripande IT-strategi samt strategier för IT-säkerhet saknas i dagsläget. Kommunen ligger dock i startgroparna för upprättande av en IT-strategi.
- Olika undergrupperingar inom IT har kommit olika långt när det gäller upprättandet av teknisk dokumentation. Det finns inget strukturerat verksamhetsövergripande arbete eller någon fastställd tidsplan för upprättandet av den dokumentation som saknas.
- Beredskapsfunktionen är något som fortfarande diskuteras. Kommunen har implementerat en lösning som gör det möjligt att kalla in personal vid behov. Denna lösning bedöms ej utgöra en fullgod jourfunktion då den förutsätter att IT-personal är nåbar via personlig telefon alternativt personlig e-mail, samt att det inte finns någon uttalad planering för vilken personal som förväntas vara tillgänglig.
- Kommunikationskedjor och ansvarsförhållanden vid en händelse eller incident är fortfarande otydliga.

Kontrollfråga 1

Arbetar kommunen med IT-säkerhet på en nivå som anses tillräcklig för att förhindra interna och externa hot från att realiseras?

Observationer

- I dagsläget använder kommunen Windows 7. Planen är att klienterna i samband med inköp av ny hårdvara skall uppgraderas till Windows 10 inom ett kvartal.
- Det finns ingen separat post i IT-budgeten avsedd för IT-säkerhet.
- Det finns ingen kontrollfunktion med ansvar för IT-säkerhet. Det finns personal med kompetens inom området men ingen som bär ett uttalat ansvar.
- Man har sedan revisionen år 2016 infört kontrollpunkter för centrala system i IT-miljön genom att implementera en lösning för loggning av dessa.
- IT-miljön scannas inte efter sårbarheter. Man har dock börjat titta på en produkt för ändamålet.
- Omvärldsbevakning bedrivs genom utskick från cert.se samt genom bevakning av media och sociala medier.
- Det finns ingen strategi för kartläggning av hot avseende IT-säkerhet.
- Nätet är segmenterat, men skulle kunna segmenteras ytterligare för högre nivå av säkerhet.
- I dagsläget förlitar man sig på accesslistor i nätverks-switchar snarare än på interna brandväggar.

Rekommendationer

- Kommunen bör utöver att uppgradera klienter till Windows 10 fokusera på att uppdatera operativsystemet på de servrar som kör äldre Windows versioner. Dessa har nått ”end-of-life” från leverantören och får därmed inte längre nödvändiga säkerhetsuppdateringar.
- En specifik post i IT-budgeten bör avsättas för IT-säkerhet. Genom detta tillses det att inköp av produkter som avser höja IT-säkerheten inte prioriteras ner till förmån för andra inköp.
- IT-miljön bör regelbundet scannas efter sårbarheter. Sårbarhetsscanning ger kommunen möjlighet att upptäcka sårbarheter och därmed agera innan interna och externa hot realiseras.
- För att höja säkerheten i nätverket rekommenderas kommunen att avveckla det nuvarande upplägget med accesslistor i switchar och istället placera interna brandväggar mellan olika zoner/segment.

Kontrollfråga 2

Har Västerviks kommun en tillräcklig beredskap för att hantera IT-incidenter?

Observationer

- Det finns inga formella styrande dokument för hantering av IT-incidenter.
- Ansvarsområden vid en IT-incident är inte fastslagna och kommunicerade.
- Kommunikationskedjor vid en IT-incident är otydliga – speciellt då det är en tekniker som upptäcker något snarare än en användare som ringer in.
- Efter att IT-kundtjänst flyttades till en annan fysisk plats än övriga IT har det uppstått ett glapp vilket kan försvåra kommunikation vid händelser och incidenter.
- Kommunen har gjort en ”cost-benefit” analys och utifrån denna gjort bedömningen att en IT-jour inte kan motiveras. Istället har IT-chefen konstant jour, och IT-personalen kan bli inkallad vid en händelse.
- De script som används i samband med backup har inte dokumenterats.
- Servermiljö och kataloger dokumenteras automatiskt via ett specifikt verktyg.
- Ett dokumenthanteringssystem skall köpas in.

Rekommendationer

- Styrande dokumentation för hantering av IT-incidenter behöver upprättas. Dokumentationen bör inkludera ansvarsområden och kommunikationskedjor vid en IT-incident.
- IT-kundtjänst bör sitta med övriga IT-avdelningen för att tillse effektiv hantering av händelser och incidenter. I dagsläget behöver man förlita sig på telefonkontakt för att få tag på rätt personer på IT, vilket inte anses hållbart.
- Kommunen behöver upprätta en jourfunktion med tydliga ansvarsförhållanden. Finns en sådan funktion på plats tillses det att större incidenter upptäcks och hanteras i tid.
- Att återläsa backup är en central del i hanteringen av många typer av incidenter. Kommunen bör därför utesluta personberoende gällande återläsningsförfarandet genom att tillse att backup-rutiner och script är tydligt dokumenterade, så att vem som helst på IT kan återläsa informationen.
- Kommunen bör införa en centraliserad lösning för lagring och åtkomst av dokumentation. Utöver att centraliserad lagring bidrar till att alla vet var dokumentationen finns att inhämta så ger ett sådant system en god överblick över vad som finns samt vad som behöver upprättas.

Kontrollfråga 3

Finns erforderliga styrdokument och ansvarsfördelning gällande IT-säkerhet och incidenthantering?

Observationer

- Det finns ingen formell IT-strategi, och inte heller någon dokumenterad strategi för IT-säkerheten.
- Kommunen har påbörjat en ansökningsprocess där man skall anställa personal med strategiskt ansvar för IT.
- Risken för personberoende har minskats genom att tillse att det finns minst två personer med kunskap inom respektive område inom IT.
- Under revisionen år 2016 påpekades det att rutiner och ansvarsområden bör kopplas till roller snarare än personer för att undvika personberoende. Man har dock valt att fortsätta koppla dessa till personer, vilket innebär att personberoendet i detta avseende kvarstår.
- Det finns en informationssäkerhetssamordnare, men ingen motsvarande roll för den tekniska IT-säkerheten.
- Vid socialförvaltningen finns en IT-ekonom med ansvars-områden gällande IT-säkerhet inom den förvaltningen. Liknande roller finns ej att finna inom övriga förvaltningar.
- Det har påbörjats arbeten att producera och revidera teknisk dokumentation. Detta sker dock inte enligt någon fastslagen tidsplan.

Rekommendationer

- Kommunen behöver skyndsamt upprätta saknade strategier. Dessa är nödvändiga verktyg för att sätta riktningen för ett område inom en verksamhet. De tillser att alla inom verksamheten jobbar mot samma mål och fattar rätt beslut.
- Ansvarsområden bör kopplas till roller snarare än till personer. Är ansvarsområden kopplade till personer introduceras ett personberoende som kan försvåra arbetet då en person är frånvarande eller slutar.
- Kommunen bör införa en roll som har det övergripande ansvaret för IT-säkerhetsfrågor. Detta säkerställer att IT-säkerhetsfrågor drivs inom verksamheten och inte åsidosätts på grund av resursbrister av olika slag.
- I de fall det finns personer med tilldelade ansvarsområden och kompetens inom IT-säkerhet även inom förvaltningarna så ges möjlighet att säkerställa att dessa frågor även drivs och tas i beaktning på förvaltningsnivå.
- Kommunstyrelsen bör säkerställa att IT-organisationen får den hjälp och det stöd som behövs för att man skall komma till rätta med den bristande dokumentationen. Om tiden inte finns internt, så behöver kommunen överväga att ta in en extern resurs som ansvarar för samordningen av upprättandet. Ett förslag på upprättande och uppdaterande av information finns i bilaga 2.

Bilagor

Bilaga 1 - Intervjulista
Bilaga 2 - Förslag till genomgång av informationshantering och uppdatering av dokumentation

Bilaga 1 - Intervjulista

Namn	Roll	Verksamhet
Peter Wahlin	IT-tekniker	IT-avdelningen
Jörgen Olsson	Systemägare	Socialförvaltningen
Therese Eriksson	IT-ekonom	Socialförvaltningen
Kim Brink	IT-tekniker	IT-kundtjänst
Per Larsson	Samordnare IT-infrastruktur och lagring	IT-avdelningen
Fredrik Carlsson	Informationssäkerhetssamordnare	Enheten för räddningsskydd och samhällsskydd
Lennart Nilsson	IT-chef	IT-avdelningen

Bilaga 2 - Förslag till genomgång av informations-hantering och uppdatering av dokumentation

2. Skapa övergripande standard för organisationens informationshantering

Standarden beskriver vad olika dokumenttyper skall innehålla, exempelvis:

- Versionshantering
- Dokumentansvar
- Revisonscykel

3. Processbeskrivning för hur dokumentation skall skapas, underhållas och avvecklas

Inom respektive ansvarsområde upprättas de rutiner som är nödvändiga för att leva upp till organisationens krav. Exempelvis hur kvalitetsgranskning skall utföras eller hur fastställande av dokument av olika typer utförs.

4. Säkerställ en god struktur

Struktur för dokumentation och information måste vara lättöverskådlig och lätt att hitta i även som nyanställd.

5. Inventering av befintlig information

Skapa en lista på vilken dokumentation som saknas samt vem som är ansvarig för att ta fram informationen.

Gör en prioritering!

1. Identifiera ägaransvar för samtlig information

Klargöra vem, dvs, vilken roll som är ansvarig för vilken dokumentation. Exempelvis IT-chef, tekniker och informationssäkerhetsansvarig.

6. Tidplan

Sätta en tidplan utifrån prioritering, när dokumentationen bör vara uppdaterad och reviderad.

7. Påbörja uppdatering/ revidering

Påbörja det faktiska arbetet med att uppdatera informationen

8. Klassning av dokument

Fastställ informationsklass, besluta om revisionscykelns intervall och ev. granskningsförfarande, etc.

11. Projektavslut

Avsluta projekt och överlämning till linjen.

10. Fastställande

Fastställ den information som kräver detta.

9. Granskningsförfarande

Granskning och second opinion på producerad och reviderad dokumentation.