TYRESÖ KOMMUN
Revisorerna

2013-09-06

Kommunstyrelsen

IT-verksamheten

De förtroendevalda revisorerna i Tyresö kommun har givit PwC i uppdrag att genomföra en översiktlig granskning av IT-verksamheten. Granskningsresultatet i sin helhet framgår av bifogad rapport.

Efter genomförd granskning bedömer vi att IT-verksamheten i kommunen saknar vissa viktiga komponenter för väsentliga områden, i syfte att säkerställa en ändamålsenlig IT-verksamhet. Trots detta bedömer vi att styrningen av den dagliga operationella verksamheten till stor del fungerar väl, men är inte fullt effektiviserad. Detta baseras bland annat på följande iakttagelser:

- Arbetet mellan BEST-IT och IT-enheten fungerar inte optimalt. Kommunen har även en utmaning i att förtydliga sin IT-styrning samt målbild för IT-enhetens personal.
- Avsaknad av ett antal styrande dokument inom informationssäkerhet samt en kontinuitetsplan för IT.
- Det finns en otydlighet avseende roller och ansvarsfördelning mellan IT-enheten, verksamheten och tredjepartsleverantörer. Detta innebär otydliga gränsdragningar för exempelvis supportfrågor eller vid driftavbrott vilket kan resultera i ett oönskat förväntansgap.

Vi rekommenderar att kommunen säkerställer att beslutade modeller för BEST-IT effektueras och att målbilder för personalen tydliggörs.

Kommunen bör även prioritera arbetet med att se över ett antal viktiga komponenter inom området informationssäkerhet, exempelvis en IT-kontinuitetsplan, samt att ett flertal säkerhetsdokument behöver införas i kommunen.

Vi rekommenderar även att en tydlig roll- och ansvarsfördelning mellan berörda parter inom IT-området fastställs och kommuniceras.

Revisorerna översänder rapporten och önskar skriftligt få del av nämndens yttrande med anledning av granskningsresultatet senast 2013-11-29. Yttrandet tillställs revisorerna via Tyresö kommuns kanslifunktion inom konsult- och servicekontoret.

För Tyresö kommuns revisorer

Palle Karlsson
Ordförande

För kännedom:
Kommunfullmäktiges presidium
Barn- och utbildningsnämnden
Socialnämnden

www.pwc.com/se

Tyresö kommun

Granskning av IT-verksamheten

Maj-juni 2013

tyresö kommun

pwc

Innehållsförteckning

1. Bakgrund och syfte

Inledning

Under maj och juni 2013 har PwC på uppdrag av revisionen i Tyresö kommun genomfört en översiktlig granskning av kommunens IT-verksamhet. Granskningen omfattar IT-organisationen såväl som IT-verksamheten inom ett urval av förvaltningar. Resultatet av granskningen presenteras i denna rapport.

Syfte

Uppdraget innebar att översiktligt granska IT-verksamheten för att få en förståelse för och analysera huruvida denna uppfyller det behov av IT-stöd som finns i kommunen. Granskningen fokuserar på; styrning och strategifrågor, teknologi och funktionalitet, projekt, personalaspekter såsom kompetens och bredd, samt ekonomi och uppföljning.

Revisionsfrågor

Rapporten avser att belysa följande:

1. Är användningen av resurser väl organiserad, strukturerad och kontrollerad för att ge och matcha en optimal IT-leverans och ett optimalt verksamhetsstöd?
2. Hur säkerställs IT-säkerheten?

2. Sammanfattning

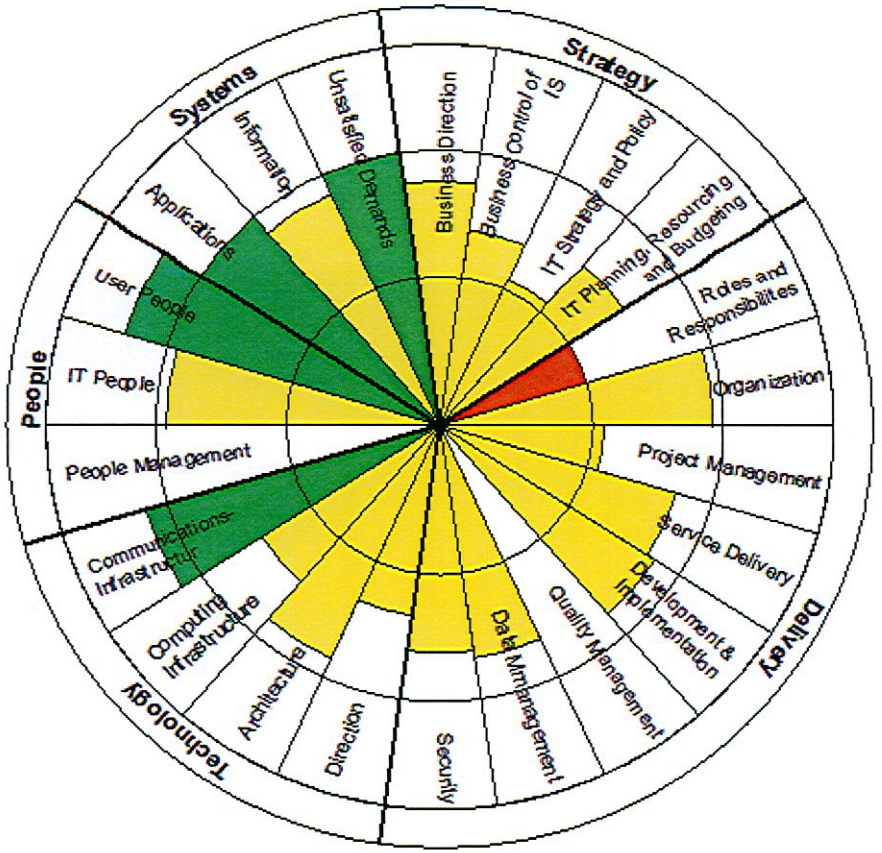
Efter genomförd granskning bedömer vi att IT-verksamheten inom kommunen saknar vissa viktiga komponenter för väsentliga områden inom IT i syfte att säkerställa en ändamålsenlig IT-verksamhet. Trots detta bedömer vi att styrningen av den dagliga operationella verksamheten till stora delar fungerar väl men är inte fullt effektiviserad. Detta baseras bland annat på följande iakttagelser:

1. Arbetet mellan BEST-IT och IT-enheten fungerar inte optimalt. Kommunen har även en utmaning i att förtydliga sin IT-styrning samt målbild för IT-enhetens personal.
2. Avsaknad av ett antal styrande dokument inom informationssäkerhet samt en kontinuitetsplan för IT.
3. Det finns en otydlighet avseende roller och ansvarsfördelning mellan IT-enheten, verksamheten och tredjepartsleverantörer. Detta innebär otydliga gränsdragningar för exempelvis supportfrågor eller vid driftavbrott vilket kan resultera i ett oönskat förväntansgap.

Vi rekommenderar att kommunen säkerställer att beslutade modeller för BEST-IT effektueras och att målbilder för personalen tydliggörs.

Kommunen bör även prioritera arbetet med att se över ett antal viktiga komponenter inom området informationssäkerhet, exempelvis en IT-kontinuitetsplan, samt att ett flertal säkerhetsdokument behöver införas i kommunen.

Vi rekommenderar även att en tydlig roll- och ansvarsfördelning mellan berörda parter inom IT-området fastställs och kommuniceras.



NOT: Områdena "Quality Management" och "People Management" har inte varit del av granskningen eftersom de inte är kopplade till revisionsfrågorna, därför finns ingen markerad färg i diagrammet ovan.

3. Genomförande och Metod

Under granskningen har verktyget ITM (IT Management analysis) använts. Verktyget bygger på en databas som innehåller jämförbar (s k *"good practice" och "benchmarking")* och relevant information för generell IT-verksamhet inom områdena IT-strategi, IT-leverans, teknologi, personal samt system och applikationer (se tabell nedan).

IT-strategi	Vad krävs för att säkerställa att IT-strategin stödjer verksamheten på bästa sätt? Hur ska verksamheten hantera och styra IT?
IT-leverans	Är användningen av resurser organiserad, strukturerad, analyserad och kontrollerad för att ge optimal IT-leverans och ett optimalt verksamhetsstöd? Hur mäts och värderas IT-stödet? Hur ligger kostnadsnivån i relation till värdet av IT?
Teknologi	Följs trender inom teknologi, är IT-arkitekturen effektiv och anskaffas teknologi på det mest effektiva sättet? Hur anpassningsbar är tekniken till förändrade behov och förutsättningar i verksamheten?
Personal	Hur hanteras personal i relation till IT (kompetens, attityder, relationsförmåga, processer och effektivitet)?
System och applikationer	Är applikationer och IT-system ändamålsenliga och kostnadseffektiva, ger de tillräckliga beslutsunderlag och vilka ytterligare behov finns?

Baserat på metoden ovan har respektive delområde bedömts utifrån en femgradig skala. Resultatet sammanfattas i ett cirkeldiagram, där färgerna rött, gult och grönt påvisar utfall i förhållande till ett önskvärt läge.

I bedömningen och vår slutsats har förutsättningar och omständigheter, specifika för Tyresö kommun, vägts in.

3. Genomförande och Metod

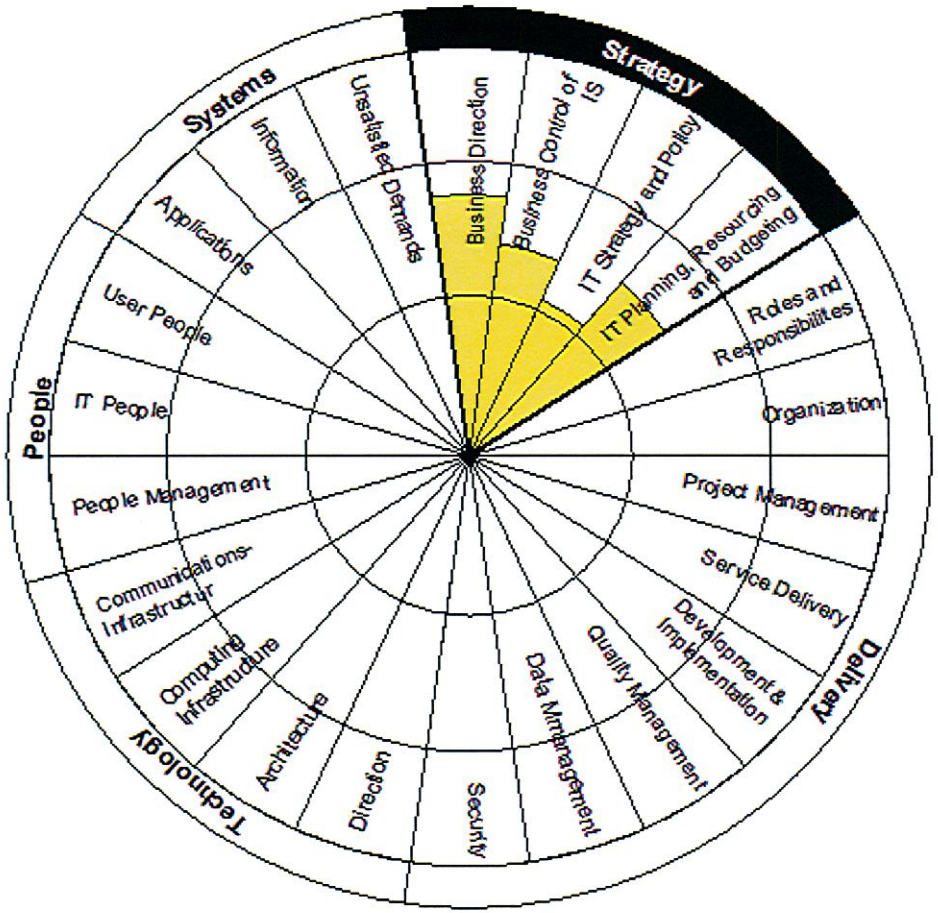
Granskningen har utförts genom intervjuer med nyckelpersoner inom Tyresö kommun, samt inläsning och genomgång av dokumentation, utredningar och annat relevant material.

Sammanlagt har åtta personer intervjuats (se tabell nedan). Urvalet har bestått av strategiska IT-personer från kommunledningen, ansvarig och operativ personal för IT-frågor samt verksamhetsrepresentanter.

Namn	Titel
Bengt Isaksson	Verksamhetskontroller och IT-ansvarig på Socialförvaltningen
Per Jacobsson	IT-tekniker
Bo Renman	Kommundirektör
Erik Sanner	Utvecklingstrateg på Barn- och utbildningsförvaltningen
Kjell Bengtsson	IT-pedagog på Barn- och utbildningsförvaltningen
Helena Franzén	Chef IT
Tomas Halvarsson	IT-chef
Torbjörn Hammar	IT-tekniker

4. Detaljerad analys

4.1.1 IT-Strategi – Översikt



4. Detaljerad analys

4.1.2 IT-Strategi - Observationer

- IT i Tyresö kommun är organiserat med en gemensam IT-driftsfunktion; IT-enheten. Sedan oktober 2012 pågår inom kommunen ett projekt, Beställarorganisation IT (BEST-IT), som har ett huvudsakligt syfte att utveckla den övergripande IT-strategin. Utifrån verksamheternas behov av befintliga och nya tjänster ska BEST-IT omsätta dessa till verklighet. Respektive förvaltning företräds i BEST-IT och ska därigenom verka för verksamhetens intressen. Vi har fått indikationer på att arbetet mellan IT-enheten, verksamheten och BEST-IT inte sker på ett optimalt sätt. Främst uppges detta bero på otydlig roll- och ansvarsfördelning mellan grupperna. Vi kan även se ett behov av en tydligare styrning inom området för att kommunen ska uppnå önskad effekt av BEST-IT.
- IT-strategin är sedan två år tillbaka ersatt med en omvärldsbevakning med specifika mål som dokumenteras i kommunplanen. Vi har noterat att kommunen har en utmaning i att förtydliga sin IT-styrning och målbild för IT-enhetens personal. En annan observation är att det saknas kommunicerade tydliga mätbara mål, vilket också bekräftas av intervjuade personer, detta kan innebära en otydlighet avseende planeringen för IT-enheten, både på kort och lång sikt. Vidare saknar kommunen en beslutad e-vision.
- Det saknas helt eller finns inte uppdaterade IT-planer för alla förvaltningar inom Tyresö kommun. De IT-planer vi har sett saknar vissa områden såsom tidplan, budget, roller och ansvarsfördelning. Det finns en översiktlig IT-plan för IT-enheten (IT-enhetens enhetsplan 2013) som gäller för 2013, däremot saknas en tydlig och dokumenterad arbetsprocess som definierar roller och ansvar för att nå aktivitetsmålen i IT-planen. IT-planen refererar även till andra styrande planer och policys som är utdaterade eller saknas. Vidare finns det en aktivitets- och projektlista för pågående projekt inom IT. Det finns även en projektplan för BEST-IT (Projektplan "BEST-IT").
- Vi har fått indikationer på avsaknad av eller brister i ett flertal styrande dokument inom området IT-säkerhet.
- Varje enskild förvaltning har en egen IT-budget och den hanteras på olika sätt. Vi har inte kunnat få en total bild av vad IT kostar för Tyresö kommun då kommunen normalt inte gör en sådan uppföljning.

4. Detaljerad analys

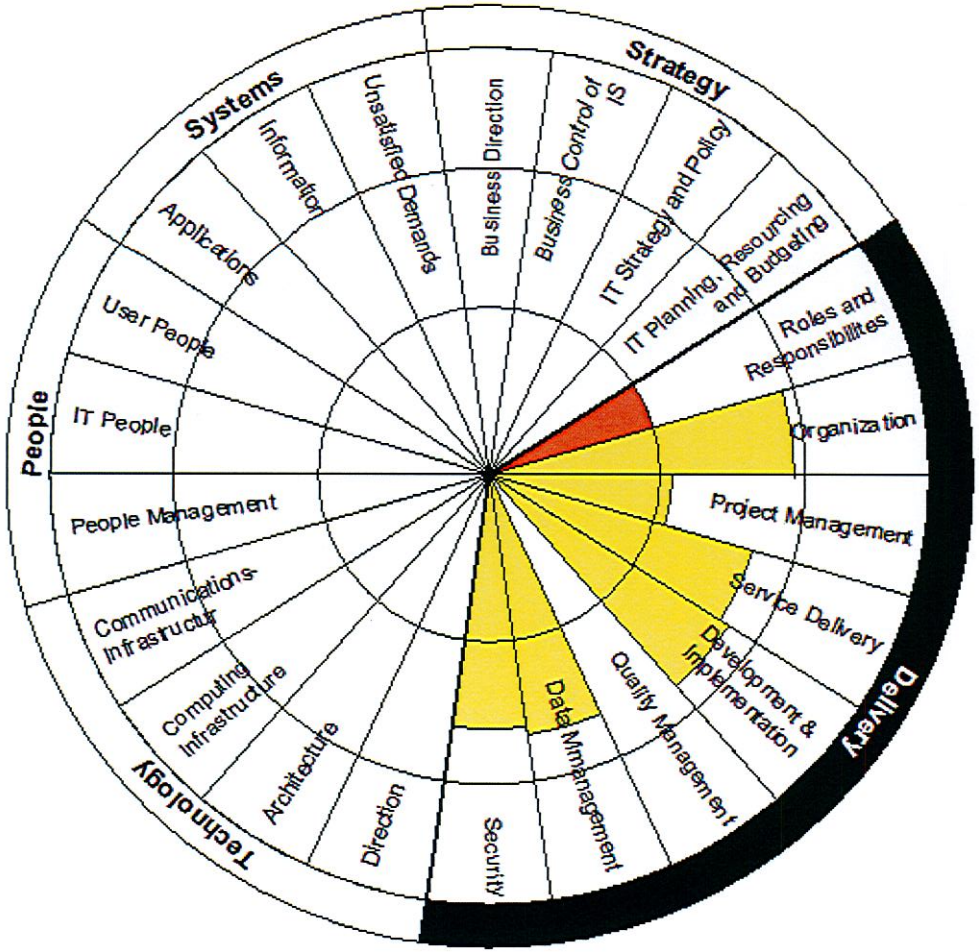
4.1.3 IT-Strategi - Rekommendationer

Vi rekommenderar att:

- kommunen fortsätter att arbeta med och utveckla BEST-IT för att säkerställa att befintliga och nya tjänster omsätts till verklighet. Det är av vikt att roll- och ansvarsfördelning mellan IT-enheten, verksamheten och BEST-IT tydliggörs. Man bör även säkerställa att kommunen som en del i projektet även utvärderar att IT-leveransen är i paritet med vad som efterfrågas av verksamheten. Förslagsvis genom att regelbundet genomföra kundenkäter för att få rätt förutsättningar att förbättra servicen mot kommunens användare. För att tydliggöra och effektuera styrningen av BEST-IT bör kommunen säkerställa att beslutade styrmodeller efterlevs.
- målbilden för IT-enheten tydliggörs och att kommunen arbetar med att uppdatera verksamhetens IT-planer och utvecklar dem med tidplaner, kostnader och förväntningar mellan verksamheten och IT. Huvudansvaret för dessa IT-planer bör ligga hos verksamheten och stämmas av med BEST-IT och IT-enheten för att få förutsättningar till att skapa en IT-plan för IT baserat på dessa planer.
- samtliga styrande dokument, policys och riktlinjer inom informationssäkerhet omgående ses över och kompletteras. En formell rutin för hur dokumenten med regelbundenhet uppdateras, hanteras och kommuniceras bör också tas fram.
- en tydlig e-vision om hur IT skall stödja verksamhet och kommuninvånare tas fram.
- kommunen genomför en översyn hur IT-kostnader sammanställs och säkerställer att alla relevanta kostnader inkluderas. En bra uppdelning är att fördela kostnader på drift, förvaltning och investering uppdelat per förvaltning, centralt för IT-enheten samt totalt för hela kommunen. Dessa kostnader ska kunna kopplas till verksamhetsplanerna och innefatta en investeringsplan. En lämplig tidshorisont för en investeringsplan kan vara tre år. I det arbetet kan kommunen med fördel även utveckla ett antal KPI:er (Key Performance Indicator) som löpande analyseras.

4. Detaljerad analys

4.2.1 IT-leverans - Översikt



4. Detaljerad analys

4.2.2 IT-leverans - Observationer

- Verksamheten upplever generellt att kommunens IT-verksamhet fungerar bra och är nöjda med servicen. IT-enheten har genomgått en omorganisation i ett led att effektivisera och förbättra verksamheten. BEST-IT och IT-enheten har regelbundna mötesformer med förvaltningar och med externa leverantörer. Dock saknas det överenskomna servicenivåer (SLA) mellan IT och kommunens förvaltningar vilket innebär att det blir svårt att mäta leveransen samt att möta förväntningar på IT.
- Såväl intervjuade personer från IT som verksamheten upplever att det finns en otydlighet avseende roller och ansvarsfördelning mellan BEST-IT, IT-enheten, verksamheten och tredjepartsleverantörer. Detta innebär otydliga gränsdragningar för exempelvis supportfrågor eller vid driftavbrott vilket kan resultera i ett oönskat förväntningsgap.
- Det finns en förteckning över systemägare/förvaltare och teknikansvariga för merparten av kommunens större verksamhetssystem, dock har vi inte erhållit någon förteckning över de kommungemensamma IT-systemen. Vidare finns en nyligen beslutad förvaltningsmodell som bland annat innehåller en beskrivning av systemförvaltares roll och ansvar.
- Vid våra intervjuer har vi noterat att det råder en osäkerhet om vilken projektmodell som används inom kommunen. En bidragande orsak till detta kan vara att kommunen nyligen antagit en ny projektmodell. Vi har även fått indikationer på att det sällan eller aldrig sker någon uppföljning eller analys på genomförda eller avslutade projekt i syfte att tydliggöra verksamhetsnyttan.
- Driften av IT-miljön sköts av kommunens egen IT-enhet och under det senaste året har det skett större uppgraderingar av den centrala IT-miljön. Det pågår ett arbete med att formalisera IT-processer då dessa saknas för bland annat förändrings- och problemhantering samt logganalyser av de centrala systemen. Avstämningar av programlicenser sker endast för centrala applikationer, för övriga programvaror/system ansvarar respektive förvaltning, vilket resulterar i att det är svårt att följa upp kostnader på en övergripande nivå.
- Det saknas en kontinuitetsplan för kommunens IT-verksamhet. Det finns en prioriteringslista över kommunens system och applikationer. Vårt översiktliga intryck är att det finns ett fysiskt och logiskt IT-skydd och den centrala IT-miljön är modern. Centrala applikationer och antivirusdefinitioner uppdateras regelbundet, för övriga programvaror/system ligger ansvaret hos respektive förvaltning.
- Det har vid intervjuer framkommit att säkerhetskopiering av data endast sparas i 14 dagar. Om verksamheten har behov av att data sparas längre tid kan detta tecknas i speciellt avtal med IT-enheten. Det är osäkert huruvida verksamheten känner till detta.

4. Detaljerad analys

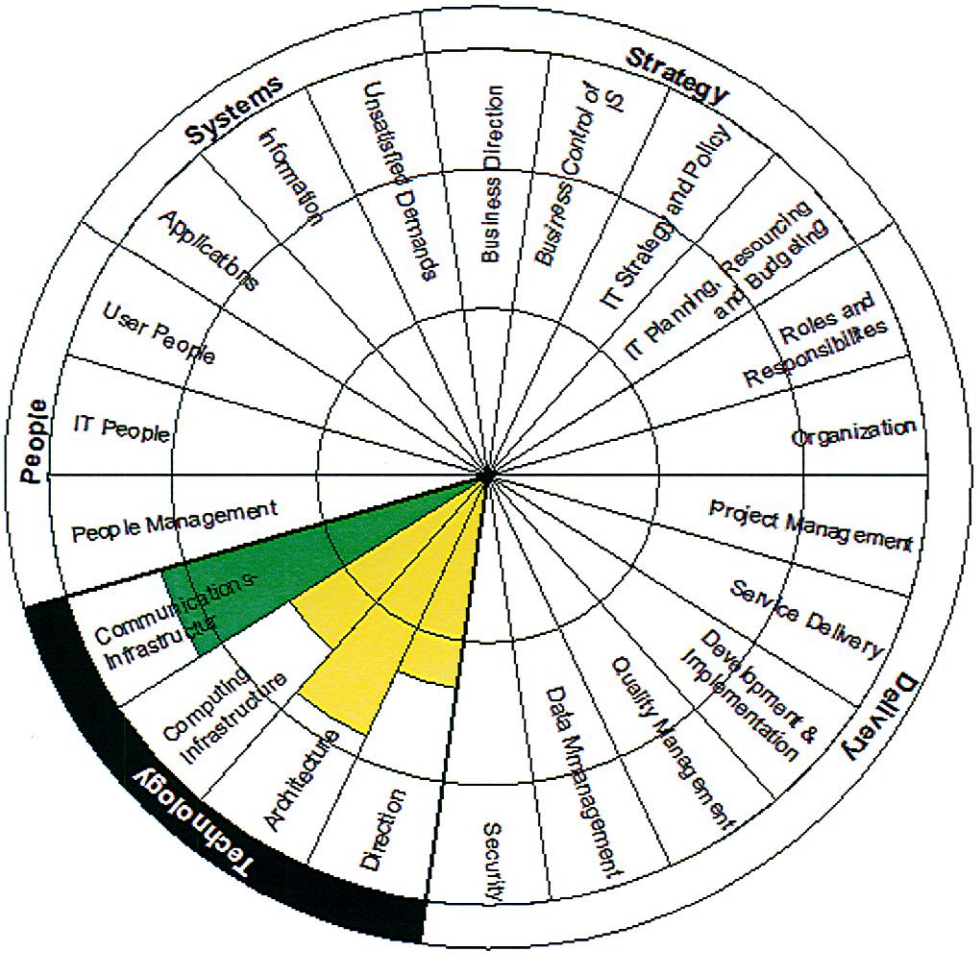
4.2.3 IT-leverans - Rekommendationer

Vi rekommenderar att:

- verksamheten prioriterar och genomför riskanalyser på sina system för att avgöra vilka som verkligen är kritiska för kommunen samt definierar ett SLA med relevanta mätpunkter för varje system som överensstämmer med verksamhetens krav och för att möjliggöra mätningar av IT-leveransen.
- ett arbete med att tydliggöra roller och ansvarsfördelningen mellan BEST-IT, IT-enheten, verksamheten och tredjepartsleverantörer initieras för att tydliggöra gränsdragningar vid supportfrågor eller driftavbrott.
- BEST-IT löpande uppdaterar förteckningen över systemförvaltare och systemägare. Vidare bör den beslutade förvaltningsmodellen kommuniceras och ett arbete med att utbilda kommunens medarbetare i förvaltningsmodellen initieras för att säkerställa att alla medarbetare är medvetna om sina roller och ansvar.
- Tyresö kommun kommunicerar den nyantagna projektmodellen till berörd personal. Kommunen bör i framtiden följa upp och utvärdera projekt löpande, både ur ett finansiellt och verksamhetsperspektiv för att få möjlighet till bättre styrning inom kommunen.
- formella IT-processer, exempelvis ITIL, utarbetas och att krav på utförande och dokumentation av tester och godkännanden för olika typer av förändringar definieras. Ansvar för tester och godkännanden bör också definieras i en sådan rutin. För att på ett effektivt sätt kunna följa upp kostnader på en kommunövergripande nivå bör man se över möjligheten att centralisera licensavstämningar och avtal.
- kommunen omgående påbörjar arbetet med att ta fram en kontinuitetsplan för IT som går i linje med kommunens katastrofplan. En åtgärdsplan för att effektivt återställa system, applikationer och processer vid en eventuell incident bör regelbundet stämmas av med verksamheten. En formell rutin för hur kontinuitetsplan för IT uppdateras och hanteras bör också tas fram.
- IT säkerställer att verksamheten är informerad om hur säkerhetskopiering sker samt att andra behov kan tillgodoses genom speciella avtal.

4. Detaljerad analys

4.3.1 Teknologi - Översikt



4. Detaljerad analys

4.3.2 Teknologi - Observationer

- Enligt uppgift har de system som IT-enheten migrerat till den nya plattformen dokumenterats. Systemdokumentation sker som en del i migreringsprocessen. System som ännu ej migrerats förefaller ha en bristande dokumentation. Vidare har vi har fått indikationer på att dokumentation av förvaltningarnas egna system kan vara bristfällig.
- Det finns ingen uttalad strategi när det gäller IT-teknik som beskriver IT-miljön ur ett mer långsiktigt perspektiv. Dock är den nya delen av IT-miljön modern, virtualiserad, standardiserad och övervakad. Vi har även fått indikationer på att processen för uppdateringar av program och säkerhetspatchar i den centrala IT-miljön brister. Exempelvis saknas regelbundna servicefönster och uppdateringar av klienter och servrar sker utan tester.
- Det genomförs inga regelbundna sårbarhetsanalyser vilket tyder på att kommunen inte har kontroll på potentiella IT-säkerhetsrisker. Vidare har kommunen ett öppet trådlöst gästnätverk utan åtkomstkontroll som enligt uppgift är nåbart från bland annat Tyresö centrum.
- Vi har låtit analysera säkerhetsinställningar och kontoadministration i kommunens katalogtjänst, Active Directory (AD). Ett utdrag av denna analys finns bifogad som en bilaga till denna rapport.

4. Detaljerad analys

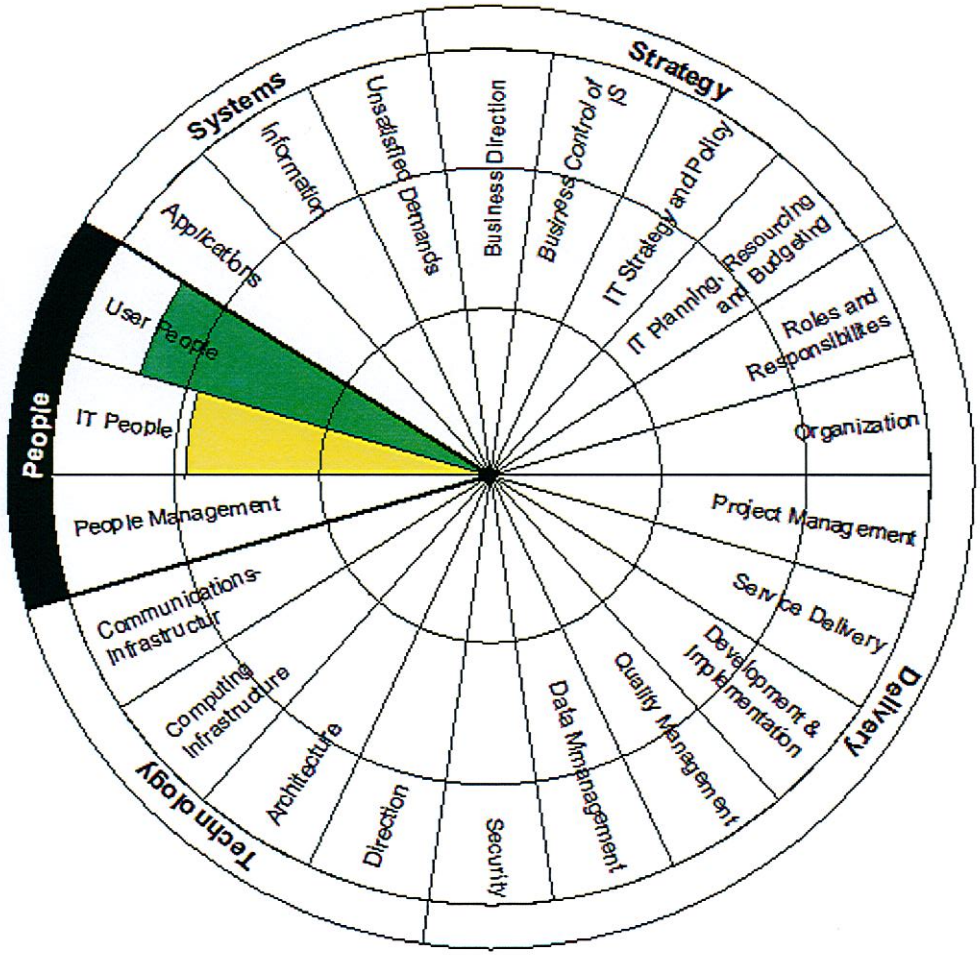
4.3.3 Teknologi - Rekommendationer

Vi rekommenderar att:

- IT-enheten dokumenterar de system som migreras till den nya plattformen enligt framtagen modell. Kommunens förvaltningarna bör säkerställa att verksamhetens dokumentation av system är fullständig och korrekt.
- en process för programuppdateringar i den centrala IT-miljön etableras. Det bör även fastställas formella dokumenterade rutiner, exempelvis ITIL, avseende hur förändringar i klient- och servermiljön får ske. Detta för att minimera eventuella driftstörningar inom IT-miljön samt minska säkerhetsrisken för kommunen.
- kontinuerliga sårbarhetsanalyser genomförs för att på så sätt säkerställa att kommunen har en hög IT-säkerhetsnivå inom samtliga förvaltningar. Om kommunen inte har ett väl fungerande säkerhetsarbete och ett strukturerat arbetssätt för att hantera IT-säkerhet är risken stor att känslig information läcker ut till obehöriga. Om en analys av det trådlösa nätverket, som säkerställer att kommunens övriga resurser är åtkomstskyddade, inte är genomfört, bör en sådan analys genomföras.

4. Detaljerad analys

4.4.1 Personal - Översikt



4. Detaljerad analys

4.4.2 Personal - Observationer

- Flertalet ur den befintliga personalen har arbetat länge inom kommunens IT-enhet. Under 2012 har fyra personer valt att avsluta sin anställning samt två personer har omorganiserats till BEST-IT. Till följd av detta kommer det under 2013 ske två nyrekryteringar till IT-enheten. Kompetensen inom gruppen är god, dock har vi vid våra intervjuer fått intrycket av att det finns nyckelpersonsberoenden på IT-enheten. Vi ser ett behov av att IT-enheten behöver förbättra sin IT-styrning och sina processer för skapa förutsättningar för att kunna utföra samma arbete som tidigare med färre resurser.
- IT har nyligen genomgått en större omorganisation samtidigt som ett omfattande arbete med plattformsbyten genomförts, både på server- och klientnivå, vilket har inneburit en period med hög arbetsbelastning, framförallt på IT-enheten. Detta har medfört att det viktiga arbetet med kompetensöverföring inom IT-enheten har eftersatts.
- Vid intervjuer framkom det att kundnöjdhetsundersökningar om IT inte genomförs regelbundet. IT uppger att undersökningar genomförs som en del av KSK:s undersökning. Dock är den generella upplevelsen av IT-stödet i kommunen enligt intervjuade personer bra. Verksamhetskunskapen inom IT-enheten bedöms vara god. Vi har dock noterat att det finns otydligheter i roller och ansvar mellan BEST-IT, IT-enheten och verksamhetens personal som till viss del arbetar med IT-frågor. Vidare använder sig IT-enheten av ett ärendehanteringssystem för att registrera ärenden som inkommer till helpdeskfunktionen. Vid våra intervjuer har det dock framkommit att delar av supportarbetet är decentraliserat då viss systemsupport ligger ute på respektive förvaltning.

4. Detaljerad analys

4.4.3 Personal - Rekommendationer

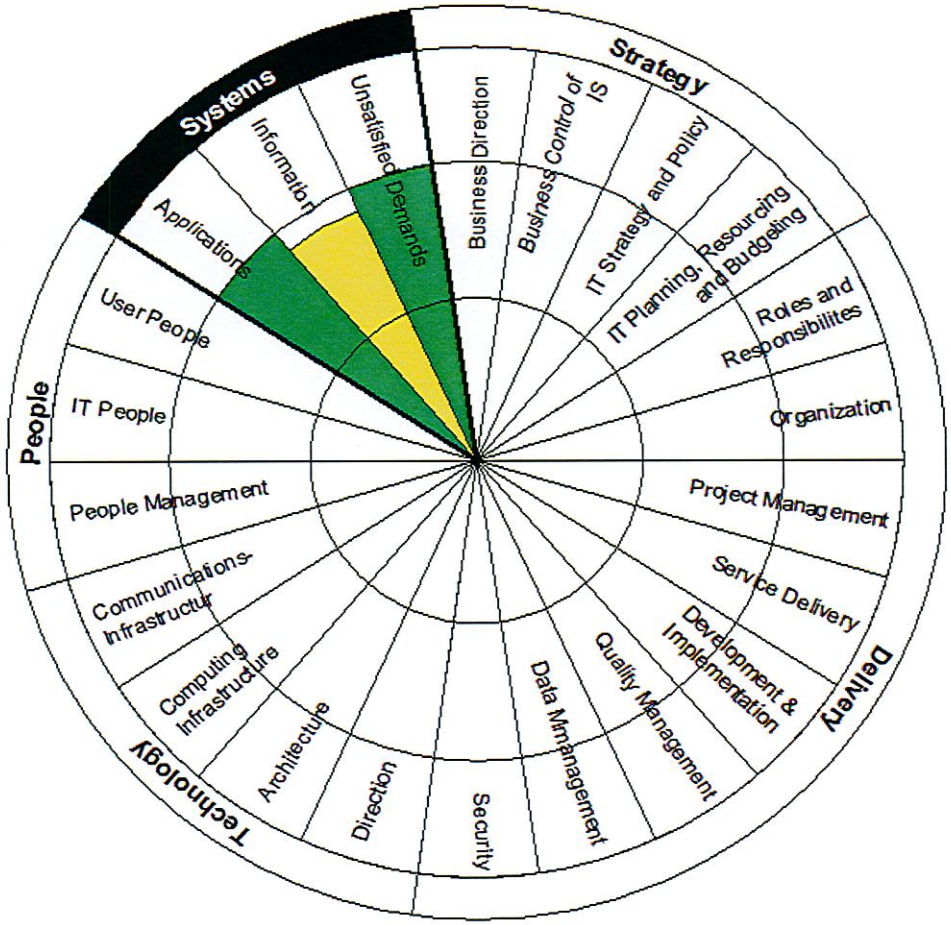
Vi rekommenderar att:

- IT-enheten genomför regelbundna kundundersökningar för att säkerställa leverans och mäta kundnöjdhet inom kommunen. Det är även viktigt att säkerställa att kunskapsspridningen inom IT-enheten fungerar och att rutiner och processer är dokumenterade för att minska nyckelpersonsberoendet.

- kommunen utarbetar en strategi och tar fram en process för hur överlämning av support på verksamhetssystem till IT-enheten ska ske. Vidare bör det tas fram tydliga roll- och ansvarsbeskrivningar mellan verksamheten, IT-enheten och BEST-IT, företrädelsevis genom tydligt definierade SLA, för att förhindra eventuella förväntningsgap.

4. Detaljerad analys

4.5.1 System och applikationer - Översikt



4. Detaljerad analys

4.5.2 System och applikationer - Observationer

- Vid plattformsbytet har ett arbete med att skapa och uppdatera en förteckning över kommunens installerade applikationer initierats. För de tre system som migrerats finns enligt uppgift dokumentation. För de system som kvarstår att migrera saknas en uppdaterad förteckning och systemdokumentation.
- Förvaltningarna inom Tyresö kommun beslutar själva vilka system och applikationer som behövs. Vilken kundnytta system eller applikationer har kan inte mätas då undersökningar av detta aldrig genomförts.
- Efter ett beslut i Barn- och utbildningsförvaltningen (BoU) använder sig en del av verksamheten av "Google Apps" istället för de traditionella IT-hjälpmedel som IT-enheten erbjuder. Hela applikations- och supportansvaret för "Google Apps" ligger idag hos BoU. Vi har noterat att det idag saknas en definierad strategi och riktlinje för hur "Google Apps" bör hanteras inom kommunen. Vi har även noterat att "Google Apps" infördes utan förstudie eller att en konsekvensanalys genomförts.

4. Detaljerad analys

4.5.3 System och applikationer - Rekommendationer

Vi rekommenderar att kommunen:

- ser över och uppdaterar dokumentationen över sina aktuella system dess systemförvaltare.
- genomför kundundersökningar på utvalda system och applikationer för att få mätvärden för användarfunktion och systemhälsa.
- definierar och beslutar om en strategi och riktlinjer för hur verksamhetsspecifika applikationer ska hanteras inom kommunen.

5. Avslutning

Vi vill avslutningsvis ta tillfället i akt och tacka de personer som deltagit i intervjuer och bidragit med underlag till denna översyn för ett vänligt bemötande och ett gott samarbete.

Vid frågor om översynen kan Janne Swenson eller Jonas Skoglund kontaktas.

Stockholm juni 2013

Kontakt:

Janne Swenson
e-post: janne.swenson@se.pwc.com
Tel: 010-213 35 22

Jonas Skoglund
e-post: jonas.skoglund@se.pwc.com
Tel: 010-212 45 26

pwc

Tyresö kommun 2013

Bilaga 1

Baseline Security Assessment

Bakgrund till granskningen

Som en del i revisionen och granskningen av IT i Tyresö kommun har PwC genomfört en allmän bedömning av säkerheten i kommunens IT-miljö. En väl anpassad nivå på informationssäkerhet är en förutsättning för tillförlitligheten i kommunens IT-miljö och rätt säkerhetsinställningar i operativsystem (OS) är en väsentlig del för att:

- Operativsystem hanterar säkerhetsinställningar för alla användare i nätverket.
- Operativsystem innehåller känsliga användarkonton och lösenord, t ex användare med utökade behörigheter.
- Operativsystem hanterar användarnas behörigheter till katalogstrukturer och till filer.
- Felaktiga säkerhetsinställningar i operativsystem kan leda till ineffektiva kontroller i applikationerna och för datalagret.

Med hjälp av ett script har PwC testat nivån på kontroll- och säkerhetsinställningar jämfört med Center for Internet Security:s (CIS) riktlinjer. Skanningen har fokuserats på de mest väsentliga inställningarna för ett urval av servrar och ska inte ses som en fullständig analys av kommunens IT-miljö. Den server som analyserats är Active Directory domänkontrollant AD03.

Analysen som genomfördes 20 maj 2013 ger en ögonblicksbild av säkerhetsinställningar och användarkonton på servern. Nya hot och risker uppstår dagligen varför resultatet i denna granskning snabbt kan bli föråldrad.

Sammanfattning

Konton

Det finns totalt 12500 konton inom Tyresö kommun, varav 12000 av dessa är aktiva. Utav dessa konton finns ett stort antal användare, cirka 5000, som inte loggat på inom 90 dagar, vilket motsvarar 40 procent. Av dessa är det dessutom cirka 3900 konton som aldrig loggat på i systemet, vilket motsvarar över 30 procent. Det tyder på att Tyresö kommun inte har kontroll på att rätt användare har tillgång till kommunens system och att Tyresö kommun brister på att följa upp behörighetsprocessen inom kommunen.

Lösenord

Vi har även noterat att det finns ett relativt stort antal konton, 344 stycken, som är definierade att inte behöva byta lösenord överhuvudtaget, oftast gäller det system- eller specialkonton. Tyresö kommun bör analysera om konton som bör byta lösenord finns bland dessa konton och i så fall uppdatera dessa med rätt konfiguration.

Tyresö kommun har enligt analysen få tecken, sex stycken, som minimumlängd för lösenord samt ingen komplexitet aktiverad, vilket inte följer CIS riktlinjer. Denna inställning gäller, enligt uppgift från IT-enheten,

endast för skolnätet. För anställd personal inom kommunen är lösenorden längre och har högre komplexitet. Vi rekommenderar att kommunen säkerställer att säkerhetsinställningarna för anställd personal följer CIS riktlinjer och om behov föreligger förstärker dessa.

Administrativa konton och behörigheter

Vidare finns det totalt 42 konton med administrativa rättigheter. Av dessa har 12 stycken inte loggat in på 90 dagar och 20 stycken behöver aldrig byta lösenord. Tyresö kommun bör analysera om dessa konton verkligen är nödvändiga och framförallt om de innehar rätt behörighetsnivå.

För våra mest väsentliga iakttagelser och våra rekommendationer, se sammanställning nedan.

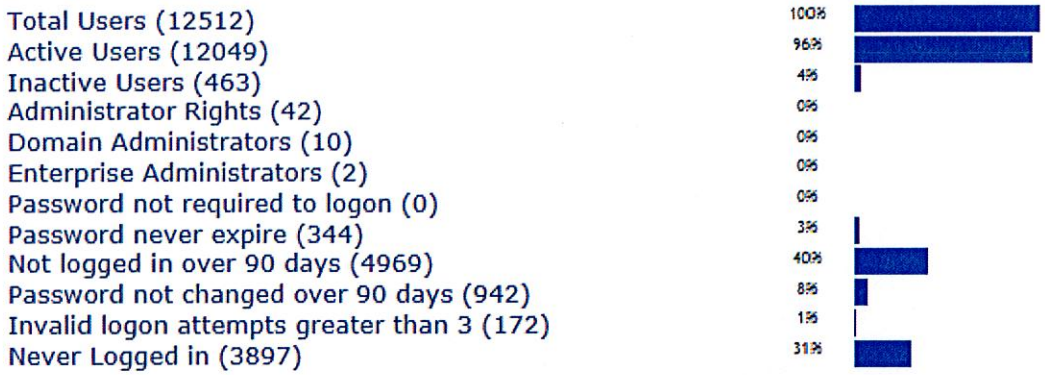
pwc

Detaljerade analyser

Analys av Baseline Security - Användare

Server

Windows Server 2008 : AD03



Väsentliga iakttagelser

40% av befintliga konton har inte loggat in på 90 dagar

Detta indikerar att processen för borttag av konton bör förstärkas. Antalet konton där lösenordet inte ändrats inom 90 dagar är lägre än antalet konton som inte loggat in under samma tidsperiod, troligtvis beror detta på att inställningen för lösenordsbyte är satt till 180 dagar.

3% av befintliga konton har "password never expire" aktiverat

För konton som har "password never expire" aktiverat sker inget tvingande byte av lösenord, vilket inte följer normala riktlinjer avseende lösenordskrav. En översyn av dessa konton bör genomföras för att utvärdera om andra konton än systemkonton har "password never expired" aktiverat.

Specialkonton med administrativa rättigheter

Totalt 42 konton har administratörsrättighet, vilket i de fall det inte avser systemkonton, ger omfattande tillgång till system och filer. Av dessa konton har:
- 12 konton inte loggat in på 90 dagar
- 20 konton inställningen "Password Never Expire" (några är sannolikt vanliga användarkonton).

31% av befintliga konton har aldrig loggat in.

Nästan 3900 konton har aldrig loggat in. Detta kan potentiellt vara en säkerhetsrisk då oanvända konton kan användas som mål vid en hacking attack.

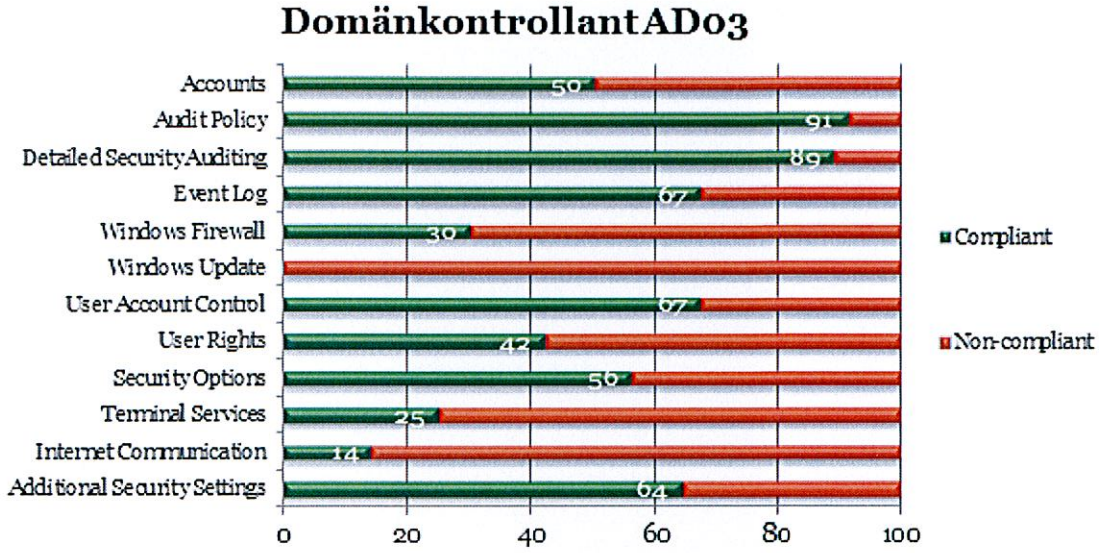
4% av befintliga konton är avaktiverade

Cirka 460 konton är avaktiverade men inte borttagna.

pwc

Analys av Baseline Security - Säkerhetsinställningar

Visar i % hur säkerhetsinställningarna överensstämmer med internationella CIS-rekommendationer.



Väsentliga iakttagelser avseende Domänkontrollant, AD03

Användarkonton: Minimum längd på lösenord
Ett längre lösenord ökar avsevärt motståndet mot en "brute force" attack.

Rekommenderat värde är ett åtta tecken långt lösenord, analysen visar sex.

Användarkonton: Tvingande lösenordbyten
Lösenord ska regelbundet bytas för att säkerställa att lösenord endast är känt för användaren som har rätt att nyttja kontot.

Rekommenderat värde är "90 dagar", analysen visar "180 dagar".

Användarkonton: Tröskelvärde för låsning av konton vid felaktiga lösenordsförsök
Denna kontroll definierar hur många gånger en användare kan skriva fel lösenord innan kontot blir låst.

Rekommenderat värde är 10 gånger. Analysen visar "0", vilket innebär att konton aldrig blir låsta.

Användarkonton: Lösenordskomplexitet
Komplexa lösenord ökar avsevärt motståndet mot en "brute force" attack genom att öka mängden av möjliga lösenordskombinationer.

Rekommenderat värde är "Enabled", analysen visar "0".

Terminal Services: Tillåt inte att lösenord sparas
Denna kontroll definierar huruvida klienten Terminal Services sparar lösenord. Om ett användarkonto med sparat lösenord blir tillgängligt för en intern eller extern "hackare" kan dessa användas för att få tillgång till aktuell och andra väsentliga servrar och databaser inom företaget.

Rekommenderat värde är "Enable", analysen visar "Registry key not found".