www.pwc.se

Revisionsrapport

Granskning av lösenordsstandard, inställningar i Active Directory och behörighetshantering inom staden.

Solna stad

Johan Friborg
Malin Lindvall

December 2019

pwc

Innehåll

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Solna stad genomfört en granskning av lösenordsstandard, inställningar i Active Directory och behörighetsgranskning inom staden.

Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande:

Har kommunstyrelsen säkerställt att Solna stads nuvarande behörighetshantering samt lösenordsstandard/kontohantering håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst?

Granskningen har skett som ett led i att följa upp en tidigare granskning som utfördes av PwC under sommaren 2018 dock med en annan revisionsfråga. Sammanfattningsvis utförde PwC då en teknisk granskning som påvisade identifierade risker kopplat till IT-säkerhet, behörighetshantering samt icke uppdaterade IT- och informations-säkerhetsdokument. Granskningen 2018 resulterade även i en rad rekommendationer som berör årlig revidering av styrdokument, incidenthanteringsprocess samt tydligare kravställning mot driftleverantör.

PwC har noterat att staden utfört och planerat åtgärder/aktiviteter i samband med byte av driftleverantör som till viss del baserats på tidigare rekommendationer i syfte att stärka IT- och informationssäkerheten.

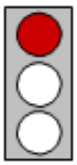
Planerade åtgärder och aktiviteter har inte tagits i beaktning i denna granskning då granskningen bör betraktas som en nulägesanalys.

Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen **ej säkerställt** att Solna stads nuvarande behörighetshantering samt lösenordsstandard håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst.

Den sammanfattande bedömningen baseras på bedömningarna av de tio kontrollmålen för granskningen, vilka redovisas i rapporten.

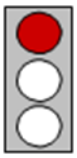
Kontrollmål 1
Det finns en utpekad ägare för stadens behörighetsmodell.

Kontrollmål 2
Staden har rutiner på plats för att säkerställa att befintliga riktlinjer och policys följs.

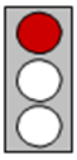


Kontrollmål 3
Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads automatgenererade konton.

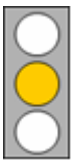
Kontrollmål 4
Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads manuellt skapade konton.



Kontrollmål 5
Stadens lösenordspolicy efterföljs.



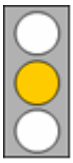
Kontrollmål 6
Staden har en god lösenordsstandard implementerad gällande exempelvis lösenordets längd och komplexitet.



Kontrollmål 7
Inga personliga konton med administrativa rättigheter som har *”password never expired”* eller där lösenordet ej har bytts ut på omotiverbart lång tid har identifierats.

Kontrollmål 8
Staden har en försvarbar mängd domänadministratörskonton.

Kontrollmål 10
Behörighetssystemet är konfigurerat så att en användare som fått nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning.



1. Inledning

1.1. Granskningsbakgrund

Av kommunallagen och god revisionssed följer att revisorerna årligen skall granska styrelser, nämnder och fasta fullmäktigeberedningar.

Kommunstyrelse och facknämnder skall förvalta och genomföra verksamheten i enlighet med fullmäktiges uppdrag, lagar och föreskrifter. För att fullgöra uppdraget måste respektive organ bygga upp system och verktyg för ledning, styrning, uppföljning, kontroll och rapportering samt säkerställa att dessa verktyg tillämpas på avsett sätt. En bristfällig styrning och kontroll kan riskera att verksamheten inte bedrivs och utvecklas på avsett sätt.

Revisorerna har uppmärksammat att risker och hot från det framväxande digitala landskapet, cyberrisker, får ökad uppmärksamhet från både företag och myndigheter. Detta främst orsakat av de senaste årens snabba digitala utveckling med följande exponering mot internet samt ökad användning av smartphones och andra bärbara enheter hos medarbetare, både privat och i yrkeslivet. Ökad aktivitet bland kriminella och andra antagonistiska aktörer bidrar även till den växande hotbilden.

Man har från såväl näringsliv som offentlig sektor insett att den hot- och riskbild som växer fram behöver bemötas. Vikten av en god behörighetshantering samt strängare lösenordskrav samt kontinuerlig revidering av användarbehörighet är en nödvändighet för att minska riskerna.

Revisorerna har i sin riskanalys för 2019 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att kommunen har en god behörighetshantering, lösenordsstandard och god kontohantering och har därför gett PwC ett uppdrag att granska området.

1.2. Syfte och revisionsfråga

Granskningen syftar till att besvara följande revisionsfråga:

Har kommunstyrelsen säkerställt att Solna stads nuvarande behörighetshantering samt lösenordsstandard/kontohantering håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst?

1.2.1. Kontrollmål

Följande kontrollmål har använts vid granskningen för att besvara revisionsfrågan:

- Det finns en utpekad ägare för stadens behörighetsmodell.
- Staden har rutiner på plats för att säkerställa att befintliga riktlinjer och policys följs.
- Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads automatgenererade konton.
- Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads manuellt skapade konton.
- Stadens lösenordspolicy efterföljs.
- Staden har en god lösenordsstandard implementerad gällande exempelvis lösenordets längd och komplexitet.
- Inga personliga konton med administrativa rättigheter som har *”password never expired”* eller där lösenordet ej har bytts ut på omotiverat lång tid har identifierats.
- Staden har en försvarbar mängd domänadministratörskonton.
- Behörighetssystemet är konfigurerat så att en användare som fått nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning.

1.3. Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kommunallagen
- IT-styrdokument

1.4. Avgränsning

I tid avgränsas granskningen till år 2019 samt till granskningens kontrollfrågor.

1.4.1. Nominerade system

I granskningen har en Domänkontrollant Server – Windows 2012 granskats gällande användarrättigheter och säkerhetsparametrar samt en Windows Server 2016 gällande säkerhetsparametrar.

1.5. Metod

Granskningen har utförts genom PwC:s tekniska koncept Baseline Security Assessment. Intervjuer med relevanta personer samt kontroll av relevant dokumentation. Genomgång av systemuppsättning genom utläsning och analys av kontoinformation i Active Directory.

PwC har testat nivån på kontroll- och säkerhetsinställningar i jämförelse med CIS ramverk (Center for Internet Security) på följande servrar:

- Windows Server 2012 – DC02
- Windows Server 2016 – PRN06

Intervjuer har genomförts med:

- Helen Holst, IT-chef - Solna stad
- Mikael Ålund, Informationssäkerhetsansvarig – Solna stad
- Asos Shafeek, Systemförvaltare AD – Solna stad
- Hans Tideborg, IT-säkerhetsansvarig – Solna stad
- Pernilla Henriksson, Kundansvarig Solna stad – Iver
- Patrik Söderström, Tekniskt ansvarig Solna stad – Iver
- Linnea Edlund, Service Desk - Dataductus

Dokumentgranskning har genomförts av dokumentation gällande policys, riktlinjer, processer, arbetsbeskrivningar och avtal tillhandahålla av Solna stad.

2. Resultat

2.1. Kontrollmål 1

Det finns en utpekad ägare för Solna stads behörighetsmodell

2.1.1. Iakttagelser

Systemförvaltaren hos Solna stad är utpekad ägare för behörighetsmodellen. Systemförvaltaren har en dokumenterad rollbeskrivning som beskriver rollens ansvarsområde, uppdrag, mål och generella arbetsuppgifter.

2.1.2. Bedömning

PwC:s bedömning är att det finns en utpekad ägare för stadens behörighetsmodell. Kontrollmålet bedöms som **uppfyllt.**

2.2. Kontrollmål 2

Staden har rutiner på plats för att säkerställa att befintliga riktlinjer och policys följs

2.2.1. Iakttagelser

Det finns övergripande rollbeskrivningar etc. i riktlinjer/policy och avtal. Det finns dock inga rutiner inkluderande instruktioner och kontroller för att säkerställa att befintliga riktlinjer och policys följs. Det arbete som de facto genomförs dokumenteras inte. Solna stad har påbörjat ett arbete att ta fram rutiner i samband med övergången från tidigare driftansvarig systemleverantör.

2.2.2. Bedömning

PwC:s bedömning är att det saknas rutiner för att säkerställa att befintliga rutiner och policys följs. Kontrollmålet bedöms som **ej uppfyllt.**

2.3. Kontrollmål 3

Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads automatgenererade konton.

2.3.1. Iakttagelser

Behörighetstilldelning, ändring och borttag av konton inom Solna stad kan ske på tre olika sätt. Anställdas behörighet styrs automatiskt av masterdatat i HR-systemet Heroma. Elevers behörighet styrs automatiskt av masterdatat i elevsystemet Procapita. Övriga behörigheter som behöver tillgång till Solna stads system men som ej finns registrerade i HR-systemen hanteras och styrs manuellt se kontrollfråga 4.

När en anställd börjar hos staden registrerar personalavdelningen personens uppgifter och organisationstillhörighet i Heroma. Genom organisationstillhörigheten får personen automatiskt de behörigheter som tillhör gruppen i AD:t. Under natten sker en automatisk synkning mot AD:t där behörigheten registreras.

När en person byter position eller slutar korrigeras detta i Heroma och behörigheten uppdateras genom den automatiska synkningen till AD:t. Om en person slutar tas rättigheterna bort och kontot sätts i karantän i 450 dagar, därefter tas det automatiskt bort. Om personen behöver ytterligare behörigheter skickas ett manuellt mail till systemförvaltaren som tilldelar ytterligare behörighet om han anser det relevant.

När en elev börjar registreras elevens uppgifter i Procapita och en automatisk avstämning sker mot Skatteverkets uppgifter. Därefter sker den automatiska synkroniseringen för tillägg, ändring och borttag på samma sätt som för anställda.

Konton hos Solna stad revideras på två olika sätt. Anställda och elevers konton, vilket är majoriteten av stadens konton revideras genom en automatisk synkning mot stadens HR-system Heroma och elevsystem mot Procapita varje natt.

För konton som genereras via Heroma och Procapita sker en automatisk rensning av avslutade konton i Active Directory. Vid avslutad anställning sätts kontot i karantän i 450 dagar och därefter tas det bort automatiskt.

2.3.2. Bedömning

PwC:s bedömning är att det finns en välfungerande behörighetstilldelning, ändring och borttag av automatiskt skapade konton. Kontrollmålet bedöms som **uppfyllt**

2.4. Kontrollmål 4

Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads manuellt skapade konton.

2.4.1. Iakttagelser

Behörighetstilldelning, ändring och borttag av konton inom Solna stad kan ske genom automatgenererade konton se kontrollfråga 3, eller genom en manuell process.

Det finns personer som behöver behörighet till Solna stads system men som inte finns registrerade i HR-systemet, exempelvis fastighetsskötare, servicekonton, driftleverantör och service desk. Dessa är manuella konton och de får sin behörighet genom IM-portalen där konton skapas, redigeras och avlutas manuellt. Registreringen till IM-portalen kan ske på flera tillvägagångssätt.

Alternativ 1 (vanligaste): personens chef kontaktar systemförvaltaren som skapar personens behörighet manuellt via IM-portalen. Systemförvaltaren kan hantera hela behörighetstilldelningen på egen hand.

Alternativ 2: det finns behöriga beställare på Solna stad som kan kontakta Dataductus via mail, telefon eller webbformulär för att beställa behörigheter. Dataductus har de behöriga beställarna registrerade i sitt system och en automatisk kontroll stämmer av att personen är behörig att göra en beställning innan Dataductus registrerar begäran.

Alternativ 3 behörighet Dataductus: Dataductus registrerar ett ärende i ärendehanteringssystemet för service desk om att de behöver skapa konton för sina egna medarbetare. Efter att systemförvaltaren har godkänt förfrågan skapar Dataductus på egen hand behörigheten.

Alternativ 4 behörighet Iver: Tekniskt ansvarig hos Iver får en begäran från personens närmsta chef om att en behörighet behöver läggas till, ändras eller tas bort. Tekniskt ansvarig skapar ett ärende i IM-portalen om begärd behörighet. I praktiken skulle Iver själva kunna skapa och hantera behörigheter, denna funktion används dock ej.

För konton som ej genererats via HR-systemen, exempelvis för fastighetsskötare och entreprenörer sker revideringen av konton manuellt av Solna stads systemförvaltare via IM-portalen (portalen för hantering av manuella konton).

Systemförvaltaren utför revidering av konton som inte går via Heroma eller Procapita ungefär en gång i månaden om personen anser att det har tillkommit många nya konton. Det finns ingen dokumenterad rutin eller process för när eller hur revidering av konton ska utföras som inte är kopplade till Heroma eller Procapita.

Användarkonton med högre behörighet eller som skapats manuellt kräver manuell genomgång vilket utförs av systemförvaltaren. Det finns ingen dokumenterad processbeskrivning för hur rensning av konton utanför Heroma och Procapita ska utföras.

Genom den intervjubaserade granskningen noterade PwC att Solna stad genomförde en granskning av tillämpning av lösenordspolicy på användarnivå den 24–26 september. I samband med granskningen noterades det att ungefär 50 konton inte hade loggat in under 2019 och ytterligare 225 konton aldrig hade loggats in varav en stor majoritet tillhörde externa leverantörer (IM-portalen).

2.4.2. Bedömning

PwC:s bedömning är att det saknas en fastställda, dokumenterade rutiner för hur revidering av manuellt skapade konton (IM-portalen) ska utföras. PwC:s samlade bedömning är att kontrollmålet **ej är uppfyllt.**

2.5. Kontrollmål 5

Stadens lösenordspolicy efterföljs

2.5.1. Iakttagelser

Enligt Solna Stads policy för lösenord bör ett lösenord vara minst tolv tecken långt. Lösenordet bör ha en hög kvalitet och bytas ut vid första påloggning.

I den tekniska BSA-analysen visar säkerhetsinställningarna att Solna stads inställningar för lösenord är åtta tecken eller längre.

2.5.2. Bedömning

PwC: bedömning är att Stadens lösenordspolicy ej efterföljs då det fortfarande finns konton med lösenordslängden åtta tecken. Kontrollmålet bedöms som **ej uppfyllt.**

2.6. Kontrollmål 6

Staden har en god lösenordsstandard implementerad gällande exempelvis lösenordets längd och komplexitet

2.6.1. Iakttagelser

IT-säkerhetsansvarig hänvisar till att Solna stad använder en tolv tecken lång lösensstandard med hög komplexitet som behöver bytas ut efter 180 dagar. För elevkonton är kraven på lösenordet lägre. Det pågår ett arbete inom Solna stad där man planerar att utöka kravet på lösenordets längd till 20 tecken i framtiden. Det finns ett inplanerat lösenordsbyte för 16 000 elever under höstlovet vecka 44.

2.6.2. Bedömning

PwC:s bedömning är att Solna stad för närvarande har en delvis god lösenordsstandard. Rekommendationen från CIS (Center for Internet Security) är att ett lösenord bör vara minst 14 tecken. PwC:s samlade bedömning är att kontrollmålet är **delvis uppfyllt.**

2.7. Kontrollmål 7

Inga personliga konton med administrativa rättigheter som har ”password never expired” eller där lösenordet ej har bytts ut på omotiverbart lång tid har identifierats

2.7.1. Iakttagelser

PwC har utfört en teknisk granskning av konton med administrativa rättigheter. Beroende på behörighetstyp har dessa delats in i tre kategorier, enterprise-, domän- och administratörskonto.

Det finns inga konton med behörigheten *Enterprise Admin* som har ”password never expired” eller där lösenordet ej har bytts ut på omotiverbart lång tid.

Det finns tio konton med behörigheten *Domain Admins* som har ”password never expired”. Av dessa konton är dock samtliga systemkonton. Det finns inget konto där lösenordet ej har bytts ut på omotiverbart lång tid.

Det finns 15 konton med behörigheten *Administrative Rights* som har ”password never expired”. Av dessa konton är dock samtliga systemkonton. Det finns sju konton där lösenordet inte har bytts ut på över 90 dagar. Samtliga av dessa konton tillhör externa leverantörer.

2.7.2. Bedömning

PwC:s bedömning är att det inte finns några personliga konton med ”password never expired” eller konton vars lösenord inte har bytts ut på omotiverbart lång tid. Kontrollmålet bedöms som **uppfyllt.**

2.8. Kontrollmål 8

Staden har en försvarbar mängd domänadministratörskonton

2.8.1. Iakttagelser

Solna stad har totalt 15 stycken domänadministratörskonton. Flertalet av kontona är systemkonton.

2.8.2. Bedömning

PwC:s bedömning är staden har en försvarbar mängd domänadministratörskonton. Kontrollmålet bedöms som **uppfyllt.**

2.9. Kontrollmål 9

Behörighetssystemet är konfigurerat så att en användare som fått nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning

2.9.1. Iakttagelser

När en ny användare får ett konto tilldelas ett systemgenererat lösenord. Detta lösenord måste användaren byta ut vid första påloggning.

När en redan befintlig användare behöver ett nytt lösenord kontaktar denna själv service desk. I majoriteten av fallen får personen ett nytt lösenord genom att identifiera sig i portalen via BankID. Vid fall där personen inte har BankID finns ett registrerat telefonnummer kopplat till samtliga användare som inte kan ändras av användaren själv. Ett nytt systemgenererat lösenord skickas i dessa fall via sms till personens telefonnummer.

När användaren får ett nytt lösenord finns det ingen funktion som tvingar användaren att byta ut lösenordet då det inte fungerar på alla system som används av Solna Stad.

2.9.2. Bedömning

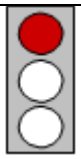
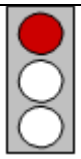
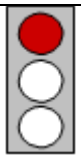
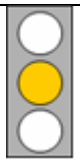
PwC:s bedömning är att behörighetssystemet är konfigurerat så att en ny användare tvingas byta till ett personligt lösenord vid första påloggning. Däremot är det inte alla av stadens system som stöttar konfigurationen vid begäran av nytt lösenord. PwC bedömer att konfigurationen används i den mån som det är möjligt. Kontrollmålet bedöms som **delvis uppfyllt.**

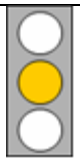
3. Bedömningar

3.1. Revisionell bedömning

Efter genomförd granskning är den sammanfattade bedömningen att kommunstyrelsen ej säkerställt att Solna stads nuvarande behörighetshantering samt lösenordsstandard håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst.

3.2. Bedömning utifrån kontrollfrågor

Kontrollmål	***Bedömning***
Det finns en utpekad ägare för stadens behörighetsmodell.	 PwC:s bedömning är att det finns en utpekad ägare för stadens behörighetsmodell. Kontrollmålet bedöms som **uppfyllt.**
Staden har rutiner på plats för att säkerställa att befintliga riktlinjer och policys följs.	 PwC:s bedömning är att det saknas rutiner för att säkerställa att befintliga rutiner och policys följs. Kontrollmålet bedöms som **ej uppfyllt.**
Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads automatgenererade konton.	 PwC:s bedömning är att det finns en väl fungerande behörighetstilldelning, ändring och borttag av automatiskt skapade konton. Kontrollmålet bedöms som **uppfyllt.**
Det finns en säker och tillförlitlig revidering, behörighetshantering och rensning av Solna stads manuellt skapade konton.	 PwC:s bedömning är att det saknas en fastställda, dokumenterade rutiner för hur revidering av manuellt skapade konton (IM-portalen) ska utföras. PwC:s samlade bedömning är att kontrollmålet **ej uppfyllt**.
Stadens lösenordspolicy efterföljs.	 PwC: bedömning är att stadens lösenordspolicy ej efterföljs då det fortfarande finns konton med lösenordslängden åtta tecken. Kontrollmålet bedöms som **ej uppfyllt.**
Staden har en god lösenordsstandard implementerad gällande exempelvis lösenordets längd och komplexitet.	 PwC:s bedömning är att Solna stad för närvarande har en delvis god lösenordsstandard. Rekommendationen från CIS (Center for Internet Security) är att ett lösenord bör vara minst 14 tecken. PwC:s samlade bedömning är att kontrollmålet är **delvis uppfyllt.**
Inga personliga konton med administrativa rättigheter som har *”password never expired”* eller där lösenordet ej har bytts ut på omotiverbart lång tid har identifierats.	 PwC:s bedömning är att det inte finns några personliga konton med ”password never expired” eller konton vars lösenord inte har bytts ut på omotiverbart lång tid. Kontrollmålet bedöms som **uppfyllt.**

Staden har en försvarbar mängd domänadministratörskonton.	 PwC:s bedömning är staden har en försvarbar mängd domänadministratörskonton. Kontrollmålet bedöms som **uppfyllt.**
Behörighetssystemet är konfigurerat så att en användare som fått nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning.	 PwC bedömer att konfigurationen används i den mån som det är möjligt. Kontollmålet bedöms som **delvis uppfyllt.**

3.3. *Rekommendationer*

Utifrån genomförd granskning lämnas följande rekommendationer.

3.3.1. Rekommendationer efter genomförd behörighetsgranskning

PwC har identifierat ett antal åtgärder som skulle leda till att behörighetshanteringen höjs till en högre nivå. Vi rekommenderar att Solna stad analyserar rekommendationerna och tillämpar dem i samband med det pågående arbetet med informationssäkerheten inom Solna stad.

3.3.2. Rekommendationer efter genomförd dokumentgranskning & intervjuer

PwC rekommenderar att Solna stad ser över behörighetshantering samt genomgång av tillhörande styrdokument för att skapa en översikt av nuvarande aktiviteter, roller och ansvarsområden.

Vi rekommenderar staden att ha uppdaterade och dokumenterade rutiner som beskriver behörighetshanteringen, vilket löpande revideras. Detta för att Solna stad, i samband med externa leverantörer skall veta vilka rutiner och riktlinjer som gäller för att skapa goda förutsättningar för att hantera eventuella risker och felaktig behörighetshantering.

Vidare rekommenderar PwC att Solna stad utför en kontinuerlig revidering av dokumentation för behörighetshantering vilket tydligt specificerar ägare, versionsnummer, ansvar och aktiviteter. Detta för att undvika icke dokumenterade aktiviteter och rutiner samt ett starkt personberoende av nyckelpersoner.

3.3.3. Övriga rekommendationer

PwC rekommenderar att hanteringen av manuella konton genom IM-portalen i högre grad standardiseras och dokumenteras. Flertalet av aktiviteterna i hanteringen av manuella konton sköts av systemförvaltaren. För att minska risken för personberoende bör dokumenterade processer tas fram för samtliga flöden i IM-portalen och för revidering av konton.

Systemförvaltaren, driftleverantören och service desk har fulla behörigheter att skapa, ändra och ta bort behörigheter. Det innebär att personer med behörigheten skulle kunna skapa ett konto, göra ändringar i systemen och plocka bort kontot utan att det upptäcks.

PwC rekommenderar därför att dessa behörigheter begränsas alternativt om detta ej är möjligt, att loggningen av dess aktiviteter följs upp löpande.

2019-12-10

Anders Hägg
Uppdragsledare

Johan Friborg
Projektledare