ÖSTERÅKERS KOMMUN
Revisorerna

Kommunstyrelsen (för yttrande)
Kommunfullmäktige (för kännedom)

## Granskning av IT -och informationssäkerhet

Vi har låtit genomföra en granskning av om Kommunstyrelsen säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen.

Efter genomförd granskning bedömer vi att Kommunstyrelsen inte helt säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen. Granskningen visar bl a att:

- Österåkers kommun har en dedikerad och kunnig teknikgrupp som målinriktat arbetar med samt ansvarar för frågor gällande IT- och informationssäkerhetsområdet i flera dimensioner.
- Det finns beredskapsfunktioner, dels i form av KiB och TiB, men även specifikt för IT- och informationssäkerhet.
- Kommunen har goda, dock informella, rutiner för backup-hantering.
- Kommunen saknar i nuläget till stor del styrande dokumentation, bl.a. återställningsplaner och informationssäkerhetspolicy. Vissa områden har styrande dokumentation, varav mycket inte längre är aktuellt, medan andra områden endast täcks av en digital applikation.
- Det finns inga dokumenterade rutiner för hur utvärderingar och förbättringar förväntas genomföras. Detta sker via informella samtal mellan berörda parter.
- Österåkers kommuns arbete präglas till stor del av manuella och ad hoc-mässiga rutiner, bl.a. vid incidenthantering.

Utifrån genomförd granskning lämnar vi följande rekommendationer till Kommunstyrelsen:

- Dokumentera huvudsakliga informationssäkerhetsprocesser.
- Ta fram en formaliserad Disaster Recovery Plan.
- Formalisera sårbarhetshanteringen med definierade processer för att upptäcka sårbarheter.
- Säkerställ att alla kommunalt anställda regelbundet genomgår utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet.
- Komplettera processkartan för incidenthantering med en tydlig incidenthanteringsplan.
- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.
- Säkerställ att återföring av lärdomar efter samtliga informationssäkerhetsincidenter görs.

- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.

Rekommendationerna är utvecklade i granskningsrapporten.

Vi översänder revisionsrapporten till Kommunstyrelsen med begäran om yttrande rörande åtgärder utifrån granskningens resultat och rekommendationer. Yttrandet emotses senast den 30 september 2021.

För Österåkers kommuns revisorer, 2021-06-16

Bengt Olin
Ordförande i kommunrevisionen

# Österåkers kommun
## IT- och informationssäkerhets-granskning

**Revisionsrapport**
Maj 2021

Linus Owman
Fredrika Jönander

# Innehållsförteckning

# 1

# Sammanfattning

# Sammanfattning

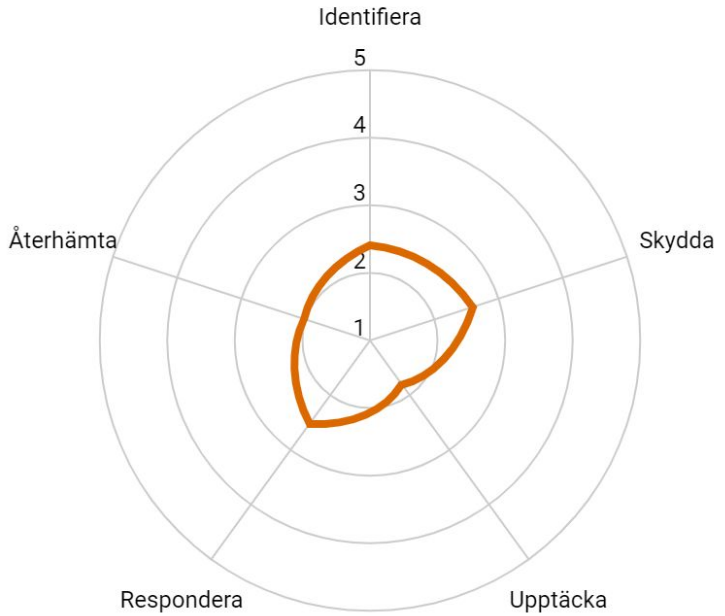
Syftet med granskningen är att bedöma om kommunstyrelsen säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen.

Efter genomförd granskning bedömer vi att kommunstyrelsen inte helt säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen. Vår bedömning är grundad i granskningen av framtagna kontrollmål, som redovisas på nästkommande sida.

Kontrollmålen är formulerade för att bedöma kommunens förmåga att identifiera säkerhetsrisker och tillgångar; skydda tillgångar; upptäcka och analysera säkerhetshändelser; hantera och kommunicera kring säkerhetshändelser samt återställa verksamheten och IT-miljön efter säkerhetshändelser och lära av dessa. Kontrollmålen är baserade på säkerhetsstandard NIST Cyber Security Framework (CSF).

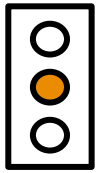
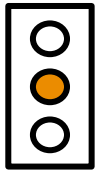
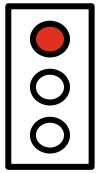
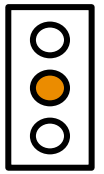
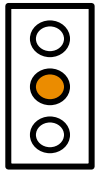
Granskningen är avgränsad till att inbegripa av kommunen utsedda representanter från relevanta befattningar som arbetar med IT- och informationssäkerhet, både ur ett operativt och strategiskt perspektiv, samt en dokumentationsanalys.

+ Österåkers kommun har en dedikerad och kunnig teknikgrupp som målinriktat arbetar med samt ansvarar för frågor gällande IT- och informationssäkerhetsområdet i flera dimensioner.
+ Det finns beredskapsfunktioner, dels i form av KiB och TiB, men även specifikt för IT- och informationssäkerhet.
+ Kommunen har goda, dock informella, rutiner för backup-hantering.
- Kommunen saknar i nuläget till stor del styrande dokumentation, bl.a. återställningsplaner och informationssäkerhetspolicy. Vissa områden har styrande dokumentation, varav mycket inte längre är aktuellt, medan andra områden endast täcks av en digital applikation.
- Det finns inga dokumenterade rutiner för hur utvärderingar och förbättringar förväntas genomföras. Detta sker via informella samtal mellan berörda parter.
- Österåkers kommuns arbete präglas till stor del av manuella och *ad hoc*-mässiga rutiner, bl.a. vid incidenthantering.




| CMMI Mognadsindex | |
|---|---|
| 5 | **Optimerad:** Kontinuerlig förbättring av processer är en del av standard operating procedures och sker regelbundet för att förbättra och effektivisera processer |
| 4 | **Hanterad:** Processer har konsekventa styrningsmetoder och utsätts för kvantitativ mätning för att värdera prestanda |
| 3 | **Definierad:** Dessa processer har ett konsekvent utförande inom organisationen med tilldelade ansvariga resurser |
| 2 | **Upprepningsbar:** Dessa processer utförs inom organisationen och har ansvariga resurser; de utförs dock inte konsekvent genom verksamheten |
| 1 | **Initial:** Dessa processer utförs “ad hoc” och saknar ett hållbart och regelbundet utförande och/eller styrning |

# Revisionell bedömning

| | | |
|---|---|---|
| ***Identifiera***<br>*Kommunen är tillräckligt bra på att identifiera, hantera, styra och övervaka tillgångar, ledningssystem, organisation, risker och tredjepartsleverantörer* | **Delvis uppfyllt** |  |
| ***Skydda***<br>*Kommunen är tillräckligt bra på att skydda tillgångar, IT-miljön och verksamheten* | **Delvis uppfyllt** |  |
| ***Upptäcka***<br>*Kommunen är tillräckligt bra på att upptäcka, övervaka, analysera och agera på anomalier och säkerhetshändelser* | **Ej uppfyllt** |  |
| ***Hantera***<br>*Kommunen är tillräckligt bra på att planera för, hantera, analysera, kommunicera kring och lära av säkerhetsincidenter* | **Delvis uppfyllt** |  |
| ***Återställa***<br>*Kommunen är tillräckligt bra att upprätthålla kontinuitet och återställa IT-miljön vid allvarliga avbrott samt hantera konsekvenser och ständigt bli bättre* | **Delvis uppfyllt** |  |

*Efter genomförd granskning bedömer vi att kommunstyrelsen **inte helt säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen**. Vår bedömning är grundad i bedömning av framtagna kontrollmål.*

# 2

# Inledning

# Bakgrund

Allt fler allvarliga cybersäkerhetsincidenter har de senaste åren drabbat såväl privat som offentlig sektor, både i Sverige och runt om i världen. En gemensam beståndsdel i flera av de mest allvarliga fallen är information som på ett eller annat sätt kommit obehörig tillhanda, antingen genom bristande rutiner och hantering eller genom yttre påverkan, i vissa fall en kombination av dem båda. MSB konstaterar att så gott som all brottslighet i det moderna samhället har koppling till IT.

All kommunal verksamhet bedrivs idag med IT-stöd. Det är därför av stor vikt att IT-stödet är driftssäkert. En av kommunernas viktigaste tillgångar är information. Kommunernas förtroende och verksamhet står således inför stora utmaningar i samband med att cyberrelaterade incidenter ökar kraftigt, medan arbetet med att stärka cybersäkerhetsförmågan ofta står stilla.

Medborgarna kommer framöver kräva allt fler digitala lösningar från sina kommuner, samtidigt som toleransen för otillgänglighet och avbrott minskar. 2017 beslutade regeringen om en ny nationell informations- och cybersäkerhetsstrategi. I denna strategi ingår att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet på alla nivåer i samhället. Kommuner berörs i allra högsta grad av denna strategi och ska ha ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete.

Ett gott informations- och cybersäkerhetsarbete är beroende av en god styrning. Ledningen ska vara engagerad och ha kunskap om informations- och cybersäkerhetsarbetet. Ledningen ska ge den strategiska inriktningen och säkerställa att det finns tillräckligt med resurser och mandat i organisationen för att kunna arbetet. Det är ledningens kravställning som styr verksamheten och det är ledningen som därmed ska säkerställa att det bedrivs ett cyber- och informationssäkrehetsarbete som är i linje med externa och interna krav. Med grund i detta ska granskningen inrikta sig på kommunstyrelsens arbete med cyber- och informationssäkerhet.

Kommunens revisorer har med hänsyn till risk och väsentlighet bedömt det angeläget att göra en granskning avseende nuläget vad gäller IT- och informationssäkerhet i kommunen.

# Bakgrund

## Syfte

Syftet med granskningen är att bedöma om kommunstyrelsen säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen. För att svara på syftet har en genomlysning genomförts med hjälp av en cybersäkerhetsmognadsmätning enligt NIST Cyber Security Framework (se 1.4 nedan). Syftet kommer att besvaras genom NIST CSF:s fem olika domäner som på ett heltäckande sätt beskriver en organisations IT- och informationssäkerhetsförmåga. Domänerna som svarar mot syftet är följande:

**Identifiera**: Kommunen är tillräckligt bra på att identifiera, hantera, styra och övervaka tillgångar, ledningssystem, organisation, risker och tredjepartsleverantörer
**Skydda**: Kommunen är tillräckligt bra på att skydda tillgångar, IT-miljön och verksamheten
**Upptäcka**: Kommunen är tillräckligt bra på att upptäcka, övervaka, analysera och agera på anomalier och säkerhetshändelser
**Hantera**: Kommunen är tillräckligt bra på att planera för, hantera, analysera, kommunicera kring och lära av säkerhetsincidenter
**Återställa**: Kommunen är tillräckligt bra på att upprätthålla kontinuitet och återställa IT-miljön vid allvarliga avbrott samt hantera konsekvenser och ständigt bli bättre nyckelpersoner.

## Avgränsning

Revisionsobjekt i granskningen är kommunstyrelsen i Österåkers kommun. Granskningen rör 2021 års verksamhet.

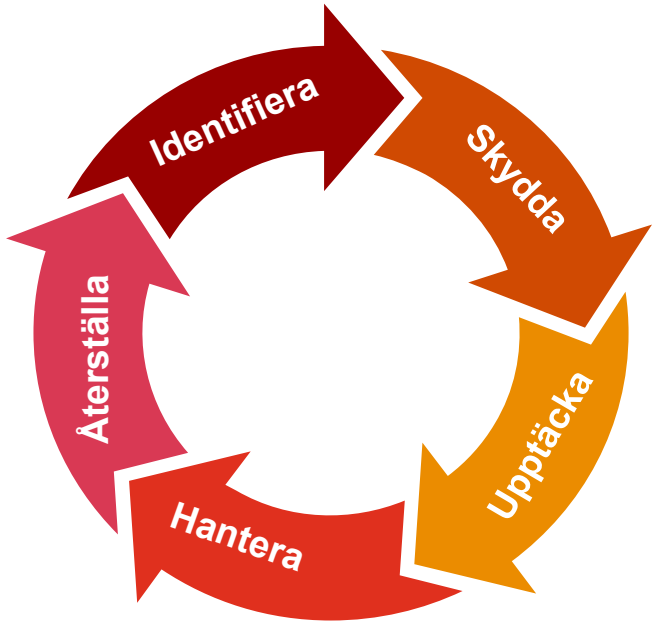
## Revisionskriterier

- Kommunallagen
- Kommuninterna styrdokument som rör granskningsområdet
- NIST Cyber Security Framework

# Metod

Granskningen utfördes med hjälp av ramverket *NIST CSF*. Ramverket utvärderar en organisations förmåga att genomföra handlingar kopplade till förmågorna **Identifiera, Skydda, Upptäcka, Hantera och Återställa** från ett resurs-, process- och teknikperspektiv. Varje område innehåller ett antal kontrollmål vars grad av uppfyllande poängsätts på en skala från 1 till 5. Ramverket har anpassats efter Österåkers kommuns förutsättningar och verksamhet. ***PwC har utvärderat Österåkers kommuns mognadsgrad beträffande följande förmågor:***

- **Identifiera**, täcker Österåkers kommuns förmåga att identifiera kritiska informationstillgångar och data, det nuvarande läget för styrning och övergripande riskhantering när det kommer till cybersäkerhet. Som ett led i detta har PwC bland annat sett till processer kopplade till riskhantering samt klassificering av tillgångar.
- **Skydda**, fokuserar på Österåkers kommuns nuvarande tillstånd när det kommer till att skydda Kommunens information samt avskräcka från hot. Denna kategori inbegriper även förmågan att hantera behörigheter och konton samt säkerhet och skyddsåtgärder kopplad till data som lagras, transporteras och bearbetas.
- **Upptäcka**, inkluderar bland annat Österåkers kommuns förmåga att övervaka IT- och säkerhetsrelaterade händelser. Detta medför bland annat möjlighet till nätverksövervakning, sökning efter skadlig kod och sårbarheter.
- **Hantera**, täcker Österåkers kommuns rutiner för åtgärdsplanering och aktiviteter kopplade till interna och externa intressenter vid en eventuell incident. Denna förmåga inkluderar bland annat forensik och incidenthantering.
- **Återställa**, relaterar till Österåkers kommuns processer för kontinuitetshantering och förmågor relaterade till resiliens och återhämtning efter hantering av incidenter. Kommunikation och publika relationer (PR) inkluderas även i denna kategori.




Granskningen baserar sig på **kvalitativa workshops tillsammans med nyckelfunktioner** inom Österåkers kommun. Personerna som deltagit har gedigen kunskap om och erfarenhet av verksamheten och dess informations- och cybersäkerhet. Vidare har granskningen inkluderat analys och **genomläsning av kommunens styrande dokument.** Granskningen genomfördes under mars till maj 2021.

# 3

# Iakttagelser och bedömningar

# Identifiera

*Iakttagelser*
Österåkers kommun har som en del av sin organisation en teknikgrupp som ansvarar för och arbetar med informations- och cybersäkerhet. Denna gruppering består bland annat av IT-chef, nätverksarkitekt och systemtekniker. Teknikgruppen har regelbundet möten där de sammanträder för att lyfta frågor, uppdateringar och nyheter kring informations- och cybersäkerhet. Vidare är det även teknikgruppen som är den primära kontaktytan för frågor inom IT-, informations- och cybersäkerhet gentemot kommunens övriga verksamheter. Utöver teknikgruppen bistår och arbetar även produktionsdirektören, tillsammans med digitaliseringsenheten, med kommunens informations- och cybersäkerhetsarbete och samtliga av kommunens skolor har en egen dedikerad IKT-resurs.

**Tillgångshantering**
Österåkers kommun har *resurser som ansvarar för tillgångshantering* i form av teknikgruppen, dock är detta ansvar endast en aspekt av flertal andra arbetsområden och uppgifter. Det finns formella processer på plats för styrning av verksamhetssystem. Det finns delvis formella processer på plats för styrning av verksamhetssystem, vilka är väl förankrade i teknikgruppen. Det saknas däremot en informationssäkerhetspolicy, eller motsvarande som dessa är förankrade i.

Gällande *inventering av hårdvara och mjukvara* finns en tydlig process för godkännande, vilket sker via attest i kommunens webbshop. Det saknas dock begränsningar i vad som kan beställas inom skolmiljön, dock kontrolleras alltid funktionaliteten hos hårdvaror i infrastrukturen. Upphandling i kommunen styrs genom att digitaliseringsenheten alltid medverkar i processen för att bland annat säkerställa att SLA-avtal tecknas.

*Behörighetshantering och kontroll av behörigheter* sköts för PC genom Microsoft System Centre och för Mac genom ACMP. Vidare är samtliga kommunala anställda begränsade i behörigheter genom att ingen anställd har administrativa rättigheter på egna enheter. Att tillägga är dock att den administrativa miljön är avsedd för PC-användare, användare av Mac-datorer har inga begränsningar gällande vad som kan laddas ned, däremot används alltid ett VPN-verktyg. Utöver detta använder kommunen Unomaly för att övervaka samt analysera alla loggar vilket även genererar larm vid avvikande beteende hos användare.

Gällande *klassning av information* har Österåkers kommun klassat majoriteten av sina system genom SKR:s verktyg KLASSA, dock återstår fortfarande cirka 20% av verksamhetssystemen. Dock har det noteras att styrning av verksamhetssystem inte sker på ett sätt som möjliggör prioritering av system utifrån hur de klassats.

**Styrning och regulatorisk efterlevnad**
Kommunen har *resurser* som ansvarar för styrning av informations- och IT-säkerhetsarbetet, som tidigare nämnt utgörs dessa till största del av kommunens teknikgrupp och det är även denna gruppering som ansvarar för hanteringen och utredningen av generella frågor avseende kommunens IT- och informationssäkerhetsarbete. Det förekommer även sammanträden genom Storstockholm av relevanta roller för att utvärdera och analysera hur kommunen omfattas av krav som leverantör av kritisk infrastruktur. Vidare är även Österåkers kommuns IT-chef styrelseledamot i ett forum för IT- och informationssäkerhet och medverkar även i Microsofts kommungrupp. Den senare genererar även checklistor i samband med regulatoriska förändringar som berör kommunen. Utöver detta finns det även en samverkansgrupp som Österåkers kommun medverkar i tillsammans med fyra andra kommuner, i denna diskuteras relevanta lagar och förordningar inom IT- och informationssäkerhetsområdet, bland annat GDPR och CloudAct. Däremot saknar kommunen verktyg för att mäta och säkerställa efterlevnad av lagstiftning och regulatoriska krav.

Gällande *styrande dokumentation* har det av intervjuer framgått att kommunen till största del undviker styrande dokumentation i form av policys, strategier och riktlinjer. Istället används till största del verktyget Trello, vilket möjliggör ett mer informellt och flexibelt förhållningssätt. Det kan med andra ord sägas att det saknas en formellt hierarkisk dokumentationsstruktur för IT- och informationssäkerhet då Österåkers kommun istället önskar att arbetssätt och rutiner ska vara integrerade i verksamheterna. För de dokument som finns används en dokumenthanteringsplan som indikerar när det är dags för revidering och uppdatering av befintlig dokumentation och det finns även ett tydligt ansvar för revidering av respektive dokument.

Det noteras att det saknas formella processer för att se till att IT- och informations-säkerhetsarbetet anpassas till kommunens verksamhetsutövning och roll som samhällsviktig aktör. Nyckelpersoner utanför IT- och informationssäkerhet är endast delaktiga i arbetet på en informell nivå. Kommunen har även endast informella processer för framtagning av strategiska inriktningar för säkerhetsarbetet som täcker in dels verksamhetsutövande, men även påverkan på medborgarna.

# Identifiera (forts.)

**Riskidentifiering och hantering**
Kommunens arbete med *riskidentifiering samt hantering av IT- och informationssäkerhets-relaterade risker* är utspritt på tre roller, vilka samverkar kring riskhantering beroende på område. Majoriteten av riskarbetet sker inom ramen för informationsklassningen via verktyget KLASSA, där det finns mallar för risk- och sårbarhetsanalyser samt för sårbarhetskartläggning. Däremot saknas det en specifik sårbarhetsprocess och det saknas även dokumentation för processerna och utfallen av sårbarhetshanteringsarbetet. Utöver arbetet som görs inom ramen för KLASSA har även riskanalyser för några utvalda och specifika system skapats. Utöver KLASSA används inget ytterligare system för riskhantering och det saknas en definierad riskaptit för kommunen. Detta bedöms enligt vad som framkommit i intervjuer vara en följd av att risktoleransen skiljer sig mellan verksamheter samt av att representant av teknikgruppen medverkar vid samtliga upphandlingar och därmed indirekt formulerar en övergripande risktolerans.

Arbetet med *omvärldsbevakning och identifiering av rådande hotbilder* är distribuerat bland teknikgruppen och vid behov tas även hjälp av kommunens befintliga leverantörer för att analysera eventuella hot. Österåkers kommun gör årligen en kommunövergripande hotanalys, men under den rådande pandemin har detta istället gjorts veckovis. Kommunen har därmed en struktur för informella diskussioner kring hotbilder, men det utförs inte några analyser i ett förebyggande syfte och inga rapporter tas fram kring hotlandskapet. Utöver detta saknar kommunen även dokumentation avseende arbetet med omvärldsbevakning och hotanalys.

**Leverantörshantering**
Som nämnts ovan medverkar en representant från teknikgruppen vid kommunens samtliga *upphandlingar*. När det kommer till att begränsa sådana risker som uppstår inom IT-miljöns leverantörskedja görs riskbedömningar och riskmatriser för samtliga planerade projekt vilka involverar leverantörer. Ansvariga roller i teknikgruppen bestämmer vilka leverantörer som ska användas för respektive projekt. IT-säkerhetsansvariga är endast inblandade i granskning av leverantörer *ad hoc*. Kommunen saknar även processer för regelbunden granskning av leverantörer. Det framgår av intervjusvar att tillgänglighet och funktionalitet prioriteras före säkerhet och därmed har kommunen vidtagit vissa åtgärder för att säkerställa leverantörers efterlevnad av tillgänglighetskrav. Vidare har kommunen även ändrat avtalsupplägg för vissa leverantörer som tidigare upplevts som problematiska och har för dessa ersatt de treåriga avtalen med ettåriga avtal.

*Bedömning*
Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att kontrollmålet är **delvis uppfyllt**. Österåkers kommun har goda rutiner och processer på plats, bland annat gällande inventering av hård- och mjukvara, samt en struktur på plats för styrning av det övergripande IT- och informationssäkerhetsarbetet. Däremot bedrivs detta till stor del ad hoc och informellt. Teknikgruppen ansvar för alla områden inom IT- och informationssäkerhet, men roller och ansvar inom gruppen är inte fullt ut formaliserade.

Det saknas en tydlig dokumentationshierarki och i dagsläget finns det både styrande dokumentation samt mer operativa rutiner och riktlinjer på Trello. Detta medför en risk för att arbetet inte bedrivs systematiskt samt att det skapas personberoenden. Det återfinns även brister inom kommunens arbete med riskhantering, delvis kopplat till att kommunen inte klassat alla system. Detta gäller främst aggregering av samtliga cybersäkerhetsrisker för enskilda verksamhetssystem, men även riskreduceringsarbetet gentemot leverantörer och utförandet av hotbildsanalyser.

Utifrån CMMI:s bedömningsskala har PwC bedömt Österåkers kommuns förmåga inom *Identifiera* till **2.4 av 5.0**, vilket innebär att kommunen har processer och resurser på plats för identifiering och hantering av cybersäkerhetsrisker men att mycket av detta arbete endast utförs informellt och ad hoc.

PwC vill särskilt fästa uppmärksamhet vid följande förbättringsområden som ligger till grund för bedömningen:

- Det saknas styrande dokumentation för IT- och informationssäkerhet.
- Kommunen har inte klassat samtliga verksamhetssystem.
- IT- och informationssäkerhetsrisker sker endast inom ramen för KLASSA.
- Kommunen ställer inga IT- eller informationssäkerhetrelaterade krav på leverantörer och genomför inte heller några granskningar av leverantörer.

# Skydda

*Iakttagelser*

**Åtkomst- och behörighetshantering**
Teknikgruppen utgör styrgrupp för *identitets- och behörighetshantering* inom kommunen. Arbetet drivs i samråd med verksamheterna som vet vilka behörigheter som krävs för de olika delarna, men det finns inte några dedikerade möten där detta finns med på dagordningen. Behörigheter är dokumenterade och det finns en process för behörighetshantering, vilket utförs genom verktyget Extense och genom förändringar i AD. Vissa användare läggs upp manuellt på verksamhetsnivå. Stickprov genomförs för att säkerställa behörigheter. I samband med att personer börjar/slutar eller byter roll finns en process för att ta bort eller ändra behörigheter och användaridentitet. Processen är manuell.

Avseende *administration av IAM* (identity and access management) har teknikgruppen igångsatt ett projekt för att robotisera tilldelningen av behörigheter där källdata hämtas från personalsystemet, men detta är ännu inte driftsatt. Verktyget Unomaly loggar användarbeteende och stämmer av mot bland annat aktuell behörighet.

*Fysisk tillträdesbegränsning* hanteras av kommunens säkerhetsavdelning och monitoreras dygnet runt. Kommunen använder taggar, larm och även kameraövervakning med realtidslarm till externt vaktbolag (trygghetslarm).

*Kommunens nätverk* är segmenterade med öppna delar för exempelvis elever samt ett administrationsnät endast för personal. Den löpande segmenteringen övervakas av regler i brandvägg och reglerna är kopplade till AD:t, vilket innebär att behörighetskontroll avläses i realtid. Det finns dock inga dokumenterade roller tilldelade inom kommunen kring hanteringen av nätverkssegmenteringen. Informellt är det välkänt att det är CTO som är ansvarig. Processen för vilka principer som reglerar hur nätverkssegmentering sker är inte dokumenterade.

**Utbildning och säkerhetsmedvetenhet**
Alla nyanställda går MSB:s *utbildning i informationssäkerhet*, något som även krävs av chefer och ledningsgrupp. Utbildningarna är obligatoriska. Det finns dock inga utbildningar som är särskilt anpassade för olika roller, varken inom IT-avdelningen, eller på olika ledarnivåer inom organisationen. Inom ramen för GDPR har kommunens dataskyddsombud genomfört vissa utbildningar med ledningsgrupp och systemförvaltare. Kommunen saknar ett utbildningsprogram för informationssäkerhet som är rollbaserat och som spårar genomförande och krav på kunskap kopplat till respektive roll.

Återrapportering till ledningsgruppen avseende utvecklingen inom IT- och informationssäkerhet, hotbilder etc sker sporadiskt. Intresset för frågorna har ökat i takt med att sanktionsbaserade regelverk införts.

**Teknisk datasäkerhet**
Avseende *dataskydd* använder kommunen sig av BitLocker på de hårddiskar som finns på lokala datorer. Servrarnas hårddiskar är okrypterade. Kommunen saknar en DLP-lösning (Data Loss Prevention), och inte heller brandväggar har en sådan funktion aktiverad. I Office365 finns dock denna funktion tillgänglig och data i Office365 kan låsas, men samtidigt innehåller Office365 endast offentlig data, vilket innebär att risken förknippad med dataförlust i denna del får anses vara låg. Principen är att all känslig data endast ska finnas i verksamhetsspecifika system och aldrig lämna dessa, men detta kan vara svårt att säkerställa om en DLP-lösning saknas. Systemägarna är ansvariga för sin egen data.

Verktyget Unomaly *övervakar trafiken*, men kan inte se innehållet i trafiken som sådan. Istället inhämtar verktyget loggar på användarbeteende som används för att bygga en baslinje för vad som är normalt användarbeteende inom ett system. Om en händelse inträffar som avviker larmar verktyget. Exempel på händelser är fler logghändelser än vanligt, okända kontonamn etc.

Systemförvaltarna är ansvariga för *gallring av data*, och det finns gallringsplaner framtagna för respektive system. All data som är i rörelse är krypterad med SSL, och utöver detta finns ytterligare varianter beroende på verksamhet (exempelvis SQL-kryptering inom skolmiljön).

**Informationssäkerhetsprocesser**
Grundkonfigurationer på serversidan bygger på templates i VMware som patchas regelbundet. Verktyget SSM används för att skicka ut installationerna. Det finns ansvariga utsedda inom teknikgruppen som har detta som sin arbetsuppgift, men rollen är inte dokumenterad. Grundkonfigurationen i klientdatorer kontrolleras regelbundet, liksom vid upphandling av nya system. Hård- och mjukvarukrav kontrolleras mot leverantör och kommunen använder verktygen SSM och Zabbix för konfigurationsövervakning.

Kommunen genomför backup på kritiska system dagligen, och veckovis på system där datan inte ändras dagligen. Backupstandarden lagras i tre månader, men kommunen har även långtidsbackup på annan lokation på databand. Kommunen har möjlighet att återställa data granulärt, alltifrån enskilda mail till en hel servermiljö.

# Skydda (forts.)

Kommunens CTO är ansvarig för *incidenthantering*. Det finns en incidentpärm med instruktioner, kontaktlistor till leverantörer etc. Återställningstider såsom MTO (Maximum Tolerable Outage) och RTO (Recovery Time Objective) är inte definierade annat än i äldre SLA, men en översyn av detta sker löpande när systemupphandlingar sker.

Servrar återskapas regelbundet i VMware-miljö. Kommunen har inte övat på återskapning av en helt ny servermiljö.

Kommunen har ingen incidentjour dygnet runt, men det finns en informell beredskap. Under intervjuer framkommer att kommunen inte har något verksamhetssystem som fordrar beredskap dygnet runt. Skulle en händelse inträffa under nattetid, exempelvis överflytt av patient från kommunen till regionen, kan journalen medföras i pappersform. Den jour som finns under dagtid omhändertar alla varningar och är sammankallande om incident inträffar. Kommunen har även en kriskommunikationsplan och möjlighet att meddela information via intranät och SMS till berörda personer (se även avsnitt “Återställa”).

*Sårbarhetsanalys* sker löpande, men utan utpekat och dokumenterat ansvar. Kommunen har dock genomfört penetrationstester med Certezza vartannat år. Sårbarheter i AD:t finns delvis tillgängligt via Microsoft Teams och Office365. Här kan även verktygen Zabbix och Unomaly nämnas.

**Skyddande teknologi**

*Analys av loggar* sker via teknikgruppen och i händelse av incidenter finns det enligt de intervjuade en process för hur logginhämtning sker. För löpande övervakning är Unomaly det verktyg som kommunen och detta ger realtidslarm. SQL-loggar övervakas av dem som har tekniskt ansvar. Kommunen saknar styrande dokument kring logghantering.

Kommunen har ingen styrning eller policy som styr flyttbar media, bortsett från en generell awareness-utbildning i samband med anställning. USB-portar är inte låsta på datorer, men det finns scanningsverktyg för USB-stickor som används. Det saknas styrning av flyttbar media kopplat till behörighet och det saknas spärrar för att personer inte ska kunna exfiltrera data. Det finns dock systemskydd i exempelvis journalsystem som omöjliggör export av data.

*Bedömning*

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att kontrollmålet är **delvis uppfyllt**. Österåkers kommun har goda rutiner och processer kopplade till backup av data och har även goda tekniska verktyg för att skydda kommunens information, bland annat genom nätverkssegmentering. Däremot utförs flera processer manuellt och endast ad hoc till följd av begränsade resurser, bland annat saknas en DLP-lösning.

Vidare saknas dokumenterat och formaliserat ansvar, för exempelvis åtkomst- och behörighetshantering. Det saknas även rollbaserade utbildningar och övningar inom IT- och informationssäkerhet. Kommunen saknar även ett utbildningsprogram med långsiktiga strategiska mål och aktiviteter.

Kommunen har inte övat på återskapning av servermiljö eller testat förmåga till återläsning eller återskapning. Det kan övergripande konstateras att det saknas systematiska och dokumenterade arbetssätt, exempelvis gällande sårbarhetsanalyser, logghantering och dokumentation kring portabel media.

Utifrån CMMI:s bedömningsskala har PwC bedömt Österåkers kommuns förmåga inom *Skydda* till **2.6 av 5.0**. Detta innebär att kommunen har processer och resurser på plats för att skydda verksamhetskritisk information och mildra tillhörande risker; dock utförs dessa inte konsekvent inom samtliga kommunala verksamheter och för samtliga system utan snarare genom informella processer.

PwC vill särskilt fästa uppmärksamhet vid följande förbättringsområden som ligger till grund för bedömningen:

- Processen för behörighetshantering är än så länge manuell.
- Österåkers kommun har inga rollbaserade övningar eller utbildningar baserat på anställdas behörighet, ansvar och arbetsroll.
- Övervakning av loggar sker manuellt.
- Kommunen saknar en DLP-lösning.

# Upptäcka

*Iakttagelser*

**Anomalier och händelser**

Kommunen använder Checkpoint som VPN-lösning. I kommunens WLAN används ett så kallat "application layer" innehållandes "Intrusion Prevention System" (IPS) och "Identity Provider" (IDP), det vill säga både viss *monitorering av sårbarheter samt en verifiering av användaridentiteter*.

För att motverka *oönskade anslutningar* av hårdvara till kommunens nätverksmiljö finns det en lista på godkänd utrustning, men det finns i nuläget inte någon spårning av otillåten hårdvara som ansluts. Istället sker styrningen med hjälp av certifikat som stänger ute de enheter som saknar dessa. Avseende trådlös anslutning finns möjligheter att finna otillåtna enheter som ansluter.

*Inträffade händelser* analyseras av teknikgruppen och även ibland i samråd med DSO, exempelvis om incidenten avser en personuppgiftsincident. Det finns inga på förhand utpekade tröskelvärden eller mallar för att bedöma incidenter, utan bedömningen sker löpande i teknikgruppen.

Incidenter som inträffar analyseras inte genom gruppering och analys, men tack vara att det ofta är samma personer som analyserar incidenterna har det ibland upptäckts mönster i olika incidenttyper. Detta beskrevs dock i intervjuer som ett mer sporadiskt arbete snarare än systematiskt.

I samband med att en incident hanterats sker en informell diskussion om hur man kunnat förhindra detta och vad som behöver förändras för att incidenten inte ska inträffa igen. Det är en avvägning mellan kostnad och skyddsnivå. Ett exempel på genomfört åtgärd är segmenteringen av nätverken. Processen för incidenthantering finns uppritad i ett flödesschema, men utöver mötesanteckningar i teknikgruppen saknas dokumentation kring hur incidenter ska hanteras.

**Kontinuerlig övervakning och förbättring av processer**

När det gäller kommunens förmåga att *upptäcka händelser och incidenter* i IT-miljön använder de, som tidigare beskrivits verktyget Unomaly för att detektera oväntade dataflöden. Kommunens brandvägg har motsvarande IDS/IPS-skydd som appliceras på den trafik som går in och ut där kommunen får indikeringar i form av larm. Utöver detta finns spam-filter och antivirus aktiverat på mail-klienterna för att bland annat upptäcka skadlig kod.

Kommunen saknar dock dedikerade resurser för monitorering av händelser. Dels för att detta sker via verktyg och dels för att det är Teknikgruppen som kollektiv som omhändertar händelser och incidenter. Det är oftast jouren som gör en första bedömning av en incident, men beroende på typ av incidenten kan ansvaret sedan flyttas till annan resurs. Teknikgruppen är även den grupp som kontinuerligt ser över det generella skyddet.

Kommunen har inget enhetligt SIEM-verktyg för att genomföra *logganalys*, men verktyget Unomaly spårar dataflöden i realtid. Kommunen har dock inget sätt att monitorera användaraktivitet i sina nätverk, utan opererar enligt devisen att inte lägga sig i. Användarbeteende styrs delvis via instruktioner, men monitorering av faktisk användaraktivitet sker ej. Här förlitar sig kommunen istället på att de verktyg som står till förfogande larmar om datatrafiken avviker från uppställda mönster.

Kommunen genomför inte regelbundet *sårbarhetsskanningar* av sin miljö, men har aktiverat de verktyg som finns från Microsoft (typ Defender), och har genomfört sårbarhetsskanningar, dock ej regelbundet. Ansvaret för resultatet av sårbarhetsskanningar och analyser omhändertas av kommunens teknikgrupp.

För att säkerställa *regelefterlevnad* använder sig kommunen främst av tekniska lösningar via skalskydd, informationsklassning (KLASSA) enligt GDPR etc. Både kommunens jurister och verksamheterna övervakar detta. Det yttersta ansvaret för frågan om personalens säkerhetsmedvetande ligger på respektive verksamhetschef. Detta är dock ej varken formaliserat eller systematiskt, och kan innebära att det inte finns en helhetssyn på regelefterlevnaden inom organisationen.

# Upptäcka (forts.)

*Bedömning*

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att kontrollmålet är **ej uppfyllt**. Österåkers kommun har goda tekniska verktyg för att upptäcka händelser som kan ha en påverkan på kommunens information. Däremot utförs flera processer endast ad-hoc till följd av begränsade resurser, bland annat saknas definierade tröskelvärden för att bedöma incidenter, metoder för att systematiskt analysera inträffade incidenter samt dedikerade resurser för monitorering av händelser och logganalys.

Utifrån CMMI:s bedömningsskala har PwC bedömt Österåkers kommuns förmåga inom Upptäcka till **1.8 av 5.0**. Denna bedömning innebär att kommunen till viss del har processer och resurser på plats för att skydda verksamhetskritisk information och mildra tillhörande risker; dock utförs dessa inte konsekvent eller systematiskt för samtliga system.

PwC vill särskilt fästa uppmärksamhet vid följande förbättringsområden som ligger till grund för bedömningen:

- Österåkers kommun saknar dedikerade resurser och verktyg för monitorering av händelser och incidenter.
- Kommunen saknar dedikerat SIEM-verktyg utan förlitar sig till stor del på manuella processer.
- Kommunen genomför inte sårbarhetsskanningar regelbundet.
- Det saknas ett formaliserat helhetsansvar och en överblick av kommunens regulatoriska efterlevnad för IT- och informationssäkerhet.

# Hantera

*Iakttagelser*

**Roller, ansvar och rutiner**
Österåkers kommun har en *beredskapsfunktion* som agerar “incident manager” när en incident inträffar. Det är denna funktion som ansvarar för incidenten och som agerar primär kontakt för all information rörande incidenten, både dagtid och kvällstid. Det saknas en dokumenterad incidenthanteringsplan, däremot finns en uppritad processkarta som inkluderar kontaktvägar och ansvarsfördelning vid incidenthantering. Vid varje inträffad incident dokumenteras detta i ett ärendehanteringssystem av kommunens ServiceDesk och det är även ServiceDesk som har instruktioner och checklistor för hur respektive typ av incident ska hanteras. Alla instruktioner för incidenthantering återfinns i Sharepoint i Office365.

Kommunen har vissa verktyg på plats som kan användas för *hantering av incidenter*, främst antivirusprogram som har möjlighet att skydda mot vissa angrepp av skadlig kod. I övrigt utförs arbetet manuellt genom att exempelvis analysera och övervaka loggar i systemet Unomaly. Därmed finns övervakning på allt som är avvikande och ovanligt, dock inkommer driftlarm på ett annat system. Loggar kan endast analyseras av utvalda roller i teknikgruppen. Strategi för vilka åtgärder som ska vidtas för att mitigera/hindra incidenter är en informell och generisk process som utgår från checklistor som finns för några incidenter, exempelvis mot virus och intrång. Processer med syfte att mildra skador från inträffade incidenter är inte automatiserade.

*Analys av inträffade incidenter* skapas som ett ärende i systemet ArtVise och IT-chef och ServiceDesk träffas månadsvis för att analysera inträffade ärenden. Utöver detta sammanträder även ServideDesk veckovis för att analysera mönster i inträffade incidenter där indikationer skapas för att sedan skickas vidare till teknikgruppen som fattar beslut om eventuella åtgärder.

Österåkers kommun har dedikerade resurser som arbetar med förbättringar efter att en incident har inträffat, återigen i form av teknikgruppen. Det är denna gruppering som ansvarar för eventuell revidering av den uppritade incidenthanterinsprocessen. Det finns dock inga rutiner för hur förbättringar och utvärderingar förväntas genomföras, utan detta sker via informella samtal mellan berörda parter. Inträffar en ny typ av incident diskuteras denna på ett teknikmöte för att analysera grundorsaken till dess inträffande.

**Kommunikation**
Österåkers kommun har en definierad roll, och ansvarsfördelningen som finns dokumenterad i kommunens kriskommunikationsplan. Under IT- och informationssäkerhetsrelaterade incidenter finns tre fördefinierade nivåer av incidenter beroende på hur verksamhetskritiskt ett system är och *kommunikationen* är anpassad därefter. Notiser kan skickas ut via kommunens applikation eller intranät. Applikationen är egenutvecklad och baseras på ett verktyg köpt av Google som kommunen kan skicka notiser till. Inträffar en incident som resulterar i att kommunens nät går ner finns alltid en laddad laptop som kan anslutas till ett mobilt nät för att få ut säkerhetsmeddelanden. Ansvar för att formulera och få ut säkerhetsmeddelanden ligger på beredskapsfunktionen, dock är det ServiceDesk som skickar ut meddelanden.

Österåkers kommun saknar en intern kommunikationsplan för hantering av IT- och informationssäkerhetrelaterade incidenter och kriser, dock framgick i intervjuer att det finns en informell process som fungerar och det finns kännedom om vilka som sköter vad.

# Hantera (forts.)

*Bedömning*
Iakttagelser från dokumentationsgranskning och intervjuer påvisar att PwC:s bedömning för kontrollmålet är **delvis uppfyllt**. Österåkers kommun har goda rutiner och processer kopplat till hantering av IT- och informationssäkerhetsincidenter, bland annat i form av en beredskapsfunktion samt en ServiceDesk med ansvar för ärendehanteringssystemet. Däremot finns det brister inom incident- och händelseanalys som kan härledas till att mycket av arbetet utförs reaktivt utefter händelser och inte i förebyggande syfte. Många processer, arbeten och initiativ sker ad hoc och det saknas beslutade rutiner och instruktioner, exempelvis en dokumenterad incidenthanteringsplan. Brister kunde även utläsas inom området förbättringar eftersom kommunen inte har några dedikerade resurser eller dokumenterade rutiner på plats gällande genomförande av utvärderingar efter inträffade incidenter.

Utifrån CMMI:s bedömningsskala har PwC bedömt Österåkers kommuns förmåga inom *Hantera* till **2.5 av 5.0**.

PwC vill särskilt fästa uppmärksamhet vid följande förbättringsområden som ligger till grund för bedömningen:

- Det saknas en dokumenterad incidenthanteringsplan.
- Det saknas rutiner för utvärdering och arbete med förbättringsområden efter inträffade händelser eller incidenter.
- Kommunen saknar en intern kommunikationsplan för hantering av IT- och informationssäkerhetrelaterade incidenter.

# Återställa

*Iakttagelser*

**Dokumentation**
I Österåkers kommun är det teknikgruppen som genomför och omhändertar *återställnings-aktiviteter*, men det saknas dock formellt dokumenterat ansvar för detta. Det saknas även en Disaster Recovery Plan, ett formellt arbete avseende *framtagning* av återställningsplaner samt testning av dessa. Kravet på framtagning av återställningsplaner är en följd av hur information inom systemet i fråga har klassats. Som tidigare nämnt har dock inte alla kommunens verksamhetssystem klassats än. Däremot har majoriteten av Österåkers kommuns system instruktioner för omstart vid behov och instruktionerna återfinns hos kommunens ServiceDesk, i händelse av att ingen i teknikgruppen skulle vara tillgänglig. Det pågår ett arbete med att formalisera prioriteringsordningen av system vid händelse av en incident I dagsläget finns denna prioritering endast i arbetsmaterial. Kommunen har som mål att under 2021 revidera och formalisera prioriteringsdokumentationen. Under 2021 ska även instruktioner och dylikt tas fram för återställning av IT-miljön, något som det i dagsläget endast finns informell kännedom om, och således ska detta tas fram med syfte att motverka personberoende.

Österåkers kommun har tidigare haft en återställningsplan, dock finns i dagsläget ingen aktuell sådan. Däremot har Österåkers kommun en sekundär lokation för återläsning och backup. På den sekundära lokation är det även möjligt att bygga upp en ny miljö om den ordinarie drifthallen skulle haverera. Återläsning av data från den sekundära lokationen är möjligt, det är dock inget som kan göras ögonblickligen utan det skulle ta en längre tid. Kommunen har enligt intervjusvar gjort bedömningen att det inte finns någon information som är så kritisk att den behöver vara tillgänglig dygnet runt. Vidare har även bedömningen gjorts att det inte behövs någon prioriteringslista av system.

**Beredskap och utvärdering**
Österåkers kommun har både en TiB (tjänsteman i beredskap) och en KiB (kommunikatör i beredskap) som en del av säkerhetsorganisationen. Det finns beredskap dygnet runt och KiB-funktionen har beredskapstelefoner och flertalet kanaler att använda sig av. Till beredskapsfunktionerna han alla typer av incidenter rapporteras och även ServiceDesk-funktionen agerar beredskap i form av omhändertagande av ärendehanteringssystemet. KiB-funktionen har en kommunikationspolicy som innehåller information om både den interna och den externa kommunikationen. Det saknas dock rutiner för utvärdering och bearbetning av lärdomar efter avslutad incident och kris.

**Kommunikation**
Kommunen har dokumenterade processer på plats för hantering av intern och extern kommunikation under kriser, både gentemot allmänheten, media samt andra kommuner. Österåkers kommun har även en kriskommunikationsplan där det framgår vilka kommunikationskanaler de använder vid händelse av kris, både analoga medel och tekniska lösningar. Kriskommunikationsplanen har dock inte testats vid exempelvis övningstillfällen där teknikgruppen medverkat under de senaste åren.

*Bedömning*
Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att kontrollmålet är **delvis uppfyllt**. Österåkers kommun har god förståelse för återställning och återskapande av IT-miljöer, men det saknas formaliserad och dokumenterad ansvarsfördelning för detta. Det saknas även en dokumenterad Disaster Recovery Plan och i dagsläget finns en prioriteringsordning för återställning endast i form av arbetsmaterial. Vidare saknas det, precis som för avsnittet *Hantera*, rutiner för utvärdering och bearbetning av lärdomar från incidenter. Däremot påvisar Österåkers kommun goda förmågor gällande kommunikation i form av en formaliserad KiB-funktion samt en kommunikationsplan och en kommunikationspolicy.

Utifrån CMMI:s bedömningsskala har PwC bedömt Österåkers kommuns förmåga inom *Återställa* till **2.0 av 5.0**. Det innebär att kommunens processer inom Återställa-förmågan utförs inom organisationen och har ansvariga resurser; däremot saknas formaliserade processer och planer på hur återställningen och återhämtningen skall ske efter en incident.

PwC vill särskilt fästa uppmärksamhet vid följande förbättringsområden som ligger till grund för bedömningen:

- Det saknas en dokumenterad Disaster Recovery Plan
- Det saknas en formaliserad och dokumenterad prioriteringsordning för återställning av system efter en inträffad incident
- Det genomförs inga regelbundna återläsningar av IT-miljön

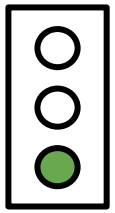
# 4

# Revisionell bedömning

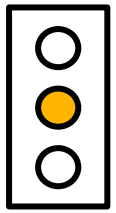
# Bedömningskriterier gällande kontrollmål

PwC gör avgränsningen att mognadsnivå 3, d.v.s. “definierad”, betraktas som tillräcklig bra och innebär att kontrollmålet är Uppfyllt, men vidhåller att det kan finnas förbättringsmöjligheter och särskilda förutsättningar som kan medföra annan bedömning, såsom att nivå 2 eller 4 kan bedömas som tillräckligt bra, samt att det är upp till organisationen att fastställa vilken nivå som ska vara ambitionen för säkerhetsarbetet.

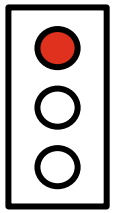
**Bedömningskriterier**



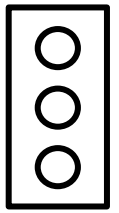
**Uppfyllt (över 3.0-5.0)**
Kontrollmålet bedöms till största delen vara uppfyllt, mindre avvikelser kan förekomma. Men verksamheten fungerar i huvudsak ändamålsenligt.



**Delvis uppfyllt (2.0-2.9)**
Kontrollmålet bedöms endast delvis vara uppfyllt, det finns en större eller flera mindre avvikelser som påverkar verksamhetens ändamålsenlighet.



**Ej uppfyllt (1.0-1.9)**
Kontrollmålet bedöms inte vara uppfyllt. Det finns avvikelser som måste åtgärdas snarast för att verksamheten ska fungera ändamålsenligt.

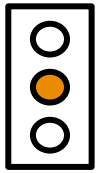
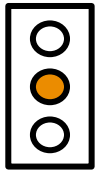
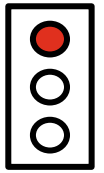
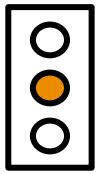
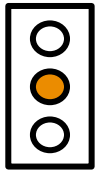


**Ej bedömt**
Kontrollmålet går ej att bedöma.

**Översättning av bedömd mognadsnivå enligt NIST CSF till bedömning av uppfyllnad av kontrollmål**

| | CMMI:s mognadsnivåer | Revisionell bedömning av uppfyllnad av kontrollmål |
|---|---|---|
| 5 | **Optimerad:** Kontinuerlig förbättring av processer är en del av standard operating procedures och sker regelbundet för att förbättra och effektivisera processer | **Uppfyllt** |
| 4 | **Hanterad:** Processer har konsekventa styrningsmetoder och utsätts för kvantitativ mätning för att värdera prestanda | **Uppfyllt** |
| 3 | **Definierad:** Dessa processer har ett konsekvent utförande inom organisationen med tilldelade ansvariga resurser | **Uppfyllt** |
| 2 | **Upprepningsbar:** Dessa processer utförs inom organisationen och har ansvariga resurser; de utförs dock inte konsekvent genom verksamheten | **Delvis uppfyllt** |
| 1 | **Initial:** Dessa processer utförs ad-hoc och saknar ett hållbart och regelbundet utförande och/eller styrning | **Ej uppfyllt** |

# Revisionell bedömning

| | | |
|---|---|---|
| ***Identifiera***<br>*Kommunen är tillräckligt bra på att identifiera, hantera, styra och övervaka tillgångar, ledningssystem, organisation, risker och tredjepartsleverantörer* | **Delvis uppfyllt** |  |
| ***Skydda***<br>*Kommunen är tillräckligt bra på att skydda tillgångar, IT-miljön och verksamheten* | **Delvis uppfyllt** |  |
| ***Upptäcka***<br>*Kommunen är tillräckligt bra på att upptäcka, övervaka, analysera och agera på anomalier och säkerhetshändelser* | **Ej uppfyllt** |  |
| ***Hantera***<br>*Kommunen är tillräckligt bra på att planera för, hantera, analysera, kommunicera kring och lära av säkerhetsincidenter* | **Delvis uppfyllt** |  |
| ***Återställa***<br>*Kommunen är tillräckligt bra att upprätthålla kontinuitet och återställa IT-miljön vid allvarliga avbrott samt hantera konsekvenser och ständigt bli bättre* | **Delvis uppfyllt** |  |

*Efter genomförd granskning bedömer vi att kommunstyrelsen **inte helt säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen**. Vår bedömning är grundad i bedömning av framtagna kontrollmål.*

# Rekommendationer

- **Dokumentera** huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat. Säkerställ att samtlig dokumentation är uppdaterad och giltig och att all dokumentation ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.
- Ta fram en **formaliserad Disaster Recovery Plan**. Säkerställ att eventuella systemägare med ansvar för att ta fram återställningsplaner är införstådda med detta ansvar.
- **Formalisera sårbarhetshanteringen** med definierade processer för hantering att upptäcka sårbarheter.
- Säkerställ att alla kommunalt anställda regelbundet genomgår **utbildningar och övningar** för att utveckla och säkerställa kompetens om informationssäkerhet. Utred huruvida det finns ett behov av rollbaserade utbildningar och övningar baserat på arbetsuppgifter, ansvar och behörigheter.
- Komplettera processkartan för incidenthantering med en **tydlig incidenthanteringsplan**.
- Formalisera **utvärderingsarbetet** efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.
- Säkerställ att **återföring av lärdomar** efter samtliga informationssäkerhetsincidenter görs genom att kravställa detta i relevant dokumentation, samt se till att det är känt inom organisationen och att det finns en dedikerad resurs som ansvarar för att detta sker.
- **Minska personberoendet** för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.

2021-06-16

Henrik Fagerlind

*Uppdragsledare*

Linus Owman

*Projektledare*

pwc.se

# 5

# Bilagor

# Bilaga 1

## Granskad dokumentation

| Dokumentnamn | Beslutad | Datum | Dokumenttyp |
|---|---|---|---|
| Österåkers mall för klassning | - | 2021-03-26 | Handlingsplan |
| Zabbix | - | - | Printscreen |
| Unomaly-Syslog | - | - | Printscreen |
| RSA Microsoft M365 | - | - | Risk- och sårbarhetsanalys |
| Riskanalys Unikum projekt 201109 | - | 2021-11-09 | Riskanalys |
| Riskanalys Unikum projekt 200520 | - | 2020-05-20 | Riskanalys |
| Risk och sårbarhetsanalys av Agressoapp | - | 2018-09-20 | Risk- och sårbarhetsanalys |
| Riktlinjer för tillämpning av integrationsmönster | - | 2018-04-23 | Riktlinje |
| Riktlinjer för säker inloggning i Österåkers kommun | - | 2018-11-14 | Riktlinje |
| Riktlinjer för namnsättning Österåkers kommun | - | 2018-04-20 | Riktlinje |
| Riktlinjer för meddelandeformat Österåkers kommun | - | 2018-03-21 | Riktlinje |
| Riktlinjer för e-förvaltning | - | 2015-2018 | Riktlinje |
| Riktlinjer för API-design | - | 2018-04-23 | Riktlinje |
| Riktlinjer för digital anslutning av externa tjänster | - | 2018-05-30 | Riktlinje |
| Processbeskrivning server och lagring Österåkers kommun | - | 2020-12-09 | Processbeskrivning |
| Processbeskrivning backup Österåkers kommun | - | 2020-12-09 | Processbeskrivning |

# Bilaga 1

## Granskad dokumentation

| Dokumentnamn | Beslutad | Datum | Dokumenttyp |
|---|---|---|---|
| Kriskommunikationsplan | - | 2020-09-24 | Plan |
| Kommunikationspolicy för Österåkers kommun | Antagen av Kommunfullmäktige 2020-12-07, § 8:8<br>Dnr: KS 2020/0187 | 2020-12-07 | Policy |
| IPAM Verktyg | - | - | Printscreen |
| Bild på informationssäkerhetsutbildning | - | - | Utdrag från intranät |
| Bild på informationssäkerhetsutbildning | - | - | Utdrag från intranät |
| Vägledning för klassificering | - | - | Vägledning |
| Incidentmall | - | 2002-09-16 | Mall |
| Bild på incidenthanteringsprocess | - | - | Printscreen |
| Ändring av konto | - | 2019-10-29 | Instruktion |
| Nytt användarkonto | - | - | Instruktion |
| Kontohantering skolan (Personal och Elever) | - | - | Instruktion |
| Kontohantering (Konsulter) | - | - | Instruktion |
| Kontohantering (externa utförare) | - | - | Instruktion |
| Avslut av konto | - | 2019-10-29 | Instruktion |

# Bilaga 2

## Intervjuade funktioner

- Produktionsdirektör
- Systemtekniker
- IT-arkitekt/CTO
- IT-chef
- Systemtekniker
- Infrastruktur- och nätverksarkitekt

# Bilaga 3

## NIST Cyber Security Framework

| NIST CSF | | | | |
|---|---|---|---|---|
| **Identifiera** | **Skydda** | **Upptäcka** | **Hantera** | **Återställa** |
| Skyddsvärden | Identitet- och accesskontroll | Avvikelser och händelser | Incidenthantering och responsplanering | Kontinuitetsplanering |
| Hotbilder och regulatoriska krav | Medvetenhet och utbildning | Kontinuerlig säkerhetsmonitorering | Kommunikation | Förbättring och åtgärder |
| Efterlevnad | Datasäkerhet | Processer för upptäckt | Händelse- och incidentanalys | Kommunikation |
| Riskbedömning | Informationsskydd processer/procedurer | | Mitigation | |
| Riskmanagementstrategi | Underhåll | | Förbättringar | |
| Leverantörers riskmanagement | Skyddsteknologi | | | |