Åda Ab

Nuläge och rekommendationer

Slutrapport för Ålands Landskapsregering

2 November 2020

Innehållsförteckning

01 Sammanfattning

Avsnittet beskriver **projektet,** dess omfattning samt konkretiserar analysens huvudsakliga resultat, det vill säga Ådas **styrkor**, **största utmaningar** och vilka **åtgärder** som är kritiska för en fortsatt utveckling av mognaden hos Åda från **nuvarande mognadsnivå**.

Granskningens bakgrund, syfte och mål

Ålands Landskapsregering har ingått ett ramavtal med KPMG Oy Ab avseende IT-revisionstjänster (ÅLR 2019/8751). Inom ramen för avtalet har en extern IT-revision avropats med syfte att granska och stödja Åda Ab:s (Åda) verksamhet, med fokus på proaktiv it-processmognad som en del av projektet Skapa förutsättningar inom IT-samordnings programmet.

KPMG:s uppdrag inom ramen för IT-revisionen var att granska nuläget samt ge rekommendationer som stöd för Åda för att uppnå en högre processmognad.

Målet med granskningen var att beskriva:

- Nuläget av IT-verksamheten, IT-risker och mognadsnivån på service management processer
- Underliggande orsaker till en viss processmognadsnivå
- Om det finns tillräckligt med kompetens och resurser inom ramen för Ådas IT:s åtagande:
  - Att kunna hantera IT drift och tillhörande styrande processer
  - Att man kan hantera driften och samtidigt utveckla den
  - Att man kan hantera sina applikationer och utveckla dessa
  - Att man kan uppnå efterlevnad av processer och informationssäkerhet
  - Om det finns tillräckligt med resurser och kompetens att
    - Kravställa IT drift och/eller upphandling
    - Förverkliga IT drift

Slutresultatet är denna rapport med observationer och rekommendationer gällande handlingsplan för att ytterligare förstärka organisationens IT förmåga till en proaktiv nivå.

Granskningens omfattning och avgränsningar

Omfattning:

För att uppfylla målet med granskningen av verksamheten, har KPMG valt majoriteten av delområdena ur en omfattande best practice operativ modell (IT Target Operating Model, IT TOM)*. Delområdena har grupperats enligt följande:

- IT-styrning
- Utveckling (infrastruktur)
- Drift
- Planering och projektstyrning
- Informationssäkerhet
- Service Management

Därtill har KPMG:s globala metod för IT riskanalys använts för att analysera och prioritera risker ur ett verksamhetsperspektiv (person-, process- och teknologirisker). Metodiken baserar sig på COSO-ERM modellen, vilken är en internationell, allmänt accepterad modell för riskstyrning och intern kontroll.

Avgränsningar:

- Granskningen omfattar Ådas verksamhet; övriga organisationer, samarbetspartners och leverantörer kan beskrivas men har inte analyserats
- Nivån på processer har inte fastställs genom testning, utan baserar sig på intervjuer och stickprov av t .ex. dokumentation, processer och övriga kontroller
- Granskningen avser att bedöma IT-verksamheten. Processmognaden granskas generellt ur ett administrativt perspektiv utan fokus på något speciellt system.
- Granskningen har utförts på en övergripande nivå inom ramen för projektets resursbudget om 130 timmar.

**) Modellen är presenterad närmare på följande sida*

Metod för evaluering av mognadsnivå

Mognadsanalysen har fokuserat på majoriteten av områden inom en best practice operativ modell i kombination med en stödjande IT riskanalys. Genom tydliga beröringspunkter, ett omfattande frågebatteri och nyttjande av ifrågavarande operativa modell, har vi genom intervjuer med nyckelpersoner tagit fram nuläget hos Åda vad beträffar IT verksamheten och Service Management.

Parallellt med intervjuer har styrdokumentation och övrig dokumentation som lyfts i samband med intervjuerna granskats. Dessa har utvärderats gentemot intervjusvar, kombinerat med jämförelse mot best practice samt KPMG:s analysverktyg.

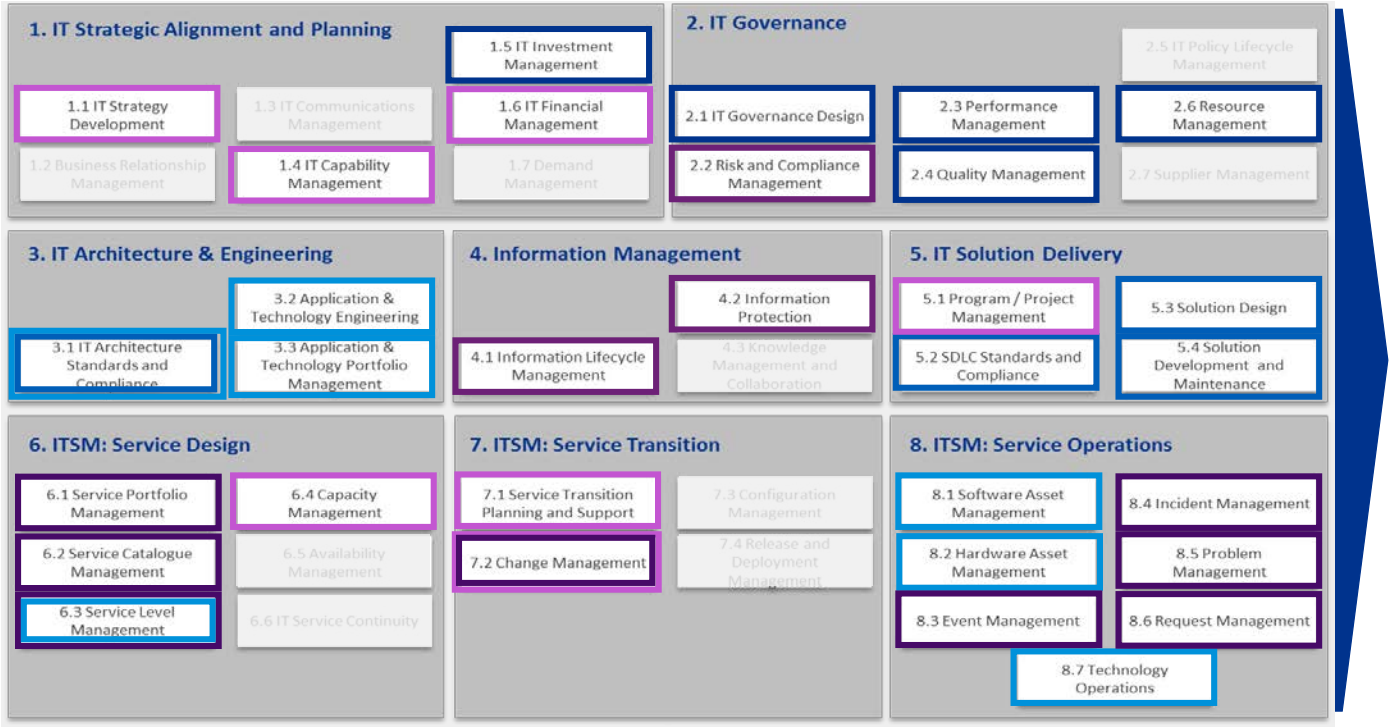
- IT-styrning
- Utveckling, infrastruktur
- Drift
- Planering och projektstyrning
- Informationssäkerhet

Strategisk verksamhetsanalys

- Service Management

Maturitetsanalys av service management processer, ITIL

Operativ modell (best practice target operating model)



Maturitetsmodell (CMM)

Nivå 5 Optimerad	• Funktionen ses som exemplarisk av jämlika organisationer. • Fokus ligger på värdeutveckling med affärsrelevanta resultatmått. • Funktionen eftersträvar ständigt innovation och utmanar verksamheten samt tillför strategiskt värde med en hållbar roll i organisationen. • Funktionen tas aktivt i beaktande av resten av verksamheten för sin förmåga.
Nivå 4 Hanterad	• Funktionens mål anpassas till organisationens behov. Utförandet av processerna sker i allmänhet felfritt. • Funktionen är integrerad i organisationen; proaktivt och strategiskt. • Prestanda mäts och hanteras med fokus på operativ duglighet och förutsägbara resultat. • Funktionen utvecklas och förbättras ständigt.
Nivå 3 Definierad	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurser.
Nivå 2 Repeterbar	• Viss förmåga finns, men disciplin för att genomföra processerna eller kommunicera konsekvent saknas ofta. • Det finns en förmåga att se kontroller men funktionen bygger på individens färdigheter.
Nivå 1 Inledande	• Minimal förmåga inom detta område med saknade eller informella processer och/eller beteenden. • Funktionen tenderar att vara reaktiv i sina handlingar med brist på styrning eller kontroll.

Sammanfattning av Ådas mognadsnivå

Nedan presenteras mognadsnivån per delområde med relaterade kriterier, samt en trendindikator för prioriteringsändamål.

Att beakta vid tolkning av maturitetsanalysen:

— Ådas mognad har granskats i förhållande till den kravställning som för tillfället ställs på Åda. Ur detta perspektiv är Åda på en relativt hög mognadsnivå och klarar av att leverera till sina kunder klart över den förväntade nivån.
— Mognadsnivån är jämförbar med motsvarande driftsleverantörer som fungerar geografiskt inom samma område med samma kravställning.
— Åda skulle ha kapacitet och förutsättningar att inom alla delområden nå en proaktiv och målstyrd nivå med mera långsiktiga och enade beställare
— En högre mognadsnivå sänker typiskt omkostnaderna genom ännu effektivare investeringar, processer, kravställningar och specifikationer enligt standardenliga mallar.

Delområde	Maturitetsnivå	Förklaring	Trend
IT-styrning	3 - DEFINIERAD Definierade och dokumenterade processer, proaktiva	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men ofta med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurs.	⇔
Utveckling, infrastruktur	2 - REPETERBAR Grundläggande processhantering, repeterbara uppgifter	• Viss förmåga finns, men disciplin för att genomföra processerna eller kommunicera konsekvent saknas ofta. • Det finns en förmåga att se kontroller men funktionen bygger på individens bästa avsikter och färdigheter.	⇔
Drift	3 - DEFINIERAD Definierade och dokumenterade processer, proaktiva	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurs.	⇔
Planering och projektstyrning	4- HANTERAD Processer är integrerade, uppmätta och kontrollerade	• Funktionens mål anpassas till organisationens behov. Utförandet av processerna sker i allmänhet felfritt. • Funktionen är integrerad i organisationen; proaktivt och strategiskt. • Prestanda mäts och hanteras med fokus på operativ duglighet och förutsägbara resultat. • Funktionen utvecklas och förbättras ständigt.	⇔
Informations-säkerhet	2 - REPETERBAR Grundläggande processhantering, repeterbara uppgifter	• Viss förmåga finns, men disciplin för att genomföra processerna eller kommunicera konsekvent saknas ofta. • Det finns en förmåga att se kontroller men funktionen bygger på individens bästa avsikter och färdigheter.	↑
Service Management	3 - DEFINIERAD Definierade och dokumenterade processer, proaktiva	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurs.	↗

Sammanfattning av observationer och rekommenderade åtgärder (1/2)

Observationer	Åtgärder
Kostnadseffektiv it-leverans förutsätter att leverantörens investeringar, kompetensutveckling och arbetssätt utvecklas för att möta en långsiktig målbild. **<u>Revisionen konstaterar:</u>** • Unikt kund-/ägarförhållande, där varken ägare eller kunder visat tydlig väg framåt • Landskapets långsiktiga digitala strategi för Ålands offentliga sektor saknas • Ägarnas strategiska målbild som tydligt beskriver de närmaste 3-5 årens krav på Åda saknas • Ägarnas beslut för standardisering och samordning saknas • Åda saknar ägarstöd för vedertagna beställarförfaranden: t.ex. kvalificerad kravställning för upphandling, klara krav på informationssäkerhet, ramverk och enhetliga processer	**Strategiska beslut för möjliggörande av mer kostnadseffektiv it-leverans** • Besluta Landskapets långsiktiga digitala strategi för Ålands offentliga sektor • Besluta ägarnas långsiktiga enade målbild för Åda, där det klart beskrivs vad som förväntas av Åda från ägarna de inkommande 3-5 åren • Säkerställa långsiktigheten gällande realisering av tagna beslut för digitala strategin och målbilden, som kan överleva politiska förändringar • Ägarnas uttalade stöd för Ådas rätt att ställa krav på sina kunder och ägare

Effektiv samordning innebär såväl teknisk utveckling som optimering av gemensamma kompetenser och gemensamma arbetssätt+. Underhåll, integrationer, övervakning och drift av kundspecifika miljöer blir dyrare i en splittrad IT-miljö
 	
<u>Revisionen konstaterar:</u>
 	
• Sådana skalfördelar i teknik, kompetens och utveckling av arbetssätt- som en samordning i normala fall för med sig - kan inte uppnås på Åland så länge ägarstyrningen sker på 1-års basis utan tydlig samordning
• Så länge kunderna väljer att äga sina tekniska miljöer och agerar som tekniska operativa beställare kan inte kunderna erhålla full nytta av skalfördelar och samordnade tjänster
	Samla ansvar och mandat för kostnadseffektiv samordning
	
	• Beslut för en standardiserad it- miljö med gemensamma tjänster, arbetssätt och resursutnyttjande
	• Utveckla kundernas beställarfunktion och styrning av sin interna it-förvaltning
	  • Åda kan fungera som drivande kraft, men kravet bör komma från ägaren om att förflytta sin egen beställarfunktion från operativ teknisk nivå till taktisk/ strategisk inriktning med fokus på digitala tjänster
	• Kunderna bör lämna över teknikansvaret för bas-it till Åda
	  • Åda bör i den utsträckning det är möjligt i nuvarande modell (kunderna äger sin IT) fortsätta att driva på och skapa kostnadseffektiva samordnade tjänster för offentliga sektorn

Sammanfattning av observationer och rekommenderade åtgärder (2/2)

Observationer	Åtgärder

Det finns få instanser som för tillfället ställer uttalade och specifika krav på Ådas kunder och därmed Ådas leverans inom informationssäkerhet och servicenivåer.
 	
<u>Revisionen konstaterar:</u>
 	
• Kunderna ställer mycket få specifika krav på Ådas servicenivåer
• Kunderna ställer mycket få specifika krav på informationssäkerhet
  • Kundens anvisningar, säkerhetspolicy-saknas till stora delar
  • Information om skyddsklasser för data som ligger i Ådas miljö saknas
• Det är mycket svårt för Åda att utveckla en högre mognadsnivå och att hitta en kostnadseffektivitet inom delområden där aktiva beställare och tydliga mål saknas.
	Styr nivån på service och informationssäkerhet
	
	• Initiera gemensam utveckling av ägarnas strategiska mål som ger:
	  • Kravställning till Åda
	  • Kravställning till ägarnas egen verksamhets implementation av policy, arbetssätt och uppföljning
	• Stötta ägarnas och övriga kunders laguppfyllnad med fortsatt utveckling av offentliga Ålands gemensamma kompetenspool inom informationssäkerhet som etablerats på Åda

För en proaktiv och effektiv it-tjänsteleverantör krävs utöver teknisk kompetens även en strategisk ledning, ständig kompetensutveckling och utveckling av arbetssätt och samverkan med kunderna.
 	
<u>Revisionen konstaterar:</u>
 	
• Åda möter motsägelsefulla budskap från ägare och beställare
  • Ägarna förväntar sig en effektiv tjänsteleverans och digitalisering
  • Beställarna ställer främst krav på operativ teknisk leverans
• Ägare och kunderna bemöter Åda mer som en operativ enhet där man gärna skulle undvika kostnaderna för tjänsteförvaltningen utöver de rent tekniska leveranserna.
• Ägarna ger inte Åda goda förutsättningar att leverera effektiva tjänster då ägare och dess beställare saknar en gemensam långsiktig målbild.
	Enade förväntningar och krav på Åda
	
	• Säkerställ en enad kravbild på Åda genom
	  • Landskapets långsiktiga digitala strategi för Ålands offentliga sektor
	  • Ägarnas långsiktiga enade målbild för Åda där det klart beskrivs vad som förväntas från ägarna de inkommande 3-5 åren
	• Utveckla funktionen för central it-förvaltning och beställarkompetens hos ägarna som har kompetens att ställa krav efter sin verksamhets långsiktiga behov och specificera vilka mål de har för sin egen verksamhet.
	• Fortsätt Ådas arbete med att utveckla it-som tjänst även för infrastruktur, support och telefoni

Sammanfattning av Ådas styrkor

Här sammanfattas de mest konkreta styrkorna hos Åda i nuläget.

- Åda strävar efter att i främsta hand använda sig av beprövad teknologi som ständigt evalueras och därmed ger Åda insikt i hur teknologin skulle fungera hos kunden
- Åda har en tydlig och fungerande uppdelning av ansvar, ledning och beslutsfattning
- Åda har en välstrukturerad modell för IT planering och projektstyrning, vilka också används vid IT utveckling
- Hantering av IT driften baserar sig på standardiserade processer, vilket gör det lättare för Åda att jobba mot tredje part, t.ex. Ådas egna eller kundens leverantörer.
- Åda har en väl fungerande process för upphandling (underliggande ramavtal) av informationsteknisk utrustning
- Planeringen av Ådas verksamhet baserar sig på en av styrelsen godkänd strategi, som bryts ner till verksamhetsplan för Åda, som i sin tur tar i beaktande kundernas behov i form av kundspecifik vägkarta. I sin helhet fungerar detta bra.
- Åda har modeller för prioritering både av kundaktiviteter och interna aktiviteter för ett budgetår i taget.
- Åda startar projekt med förstudie, på basen av vilket ett utvecklingsprojekt antingen startar eller förkastas. Detta är en bra kutym och minskar risken för misslyckande.
- Projektstyrningen överlag är på en god nivå med klara steg och klara roller både hos Åda och kunden.
- Man försöker aktivt föra över Ådas strukturella sätt att jobba t.ex. i projekt till sina kunder
- Man testar aktivt nya tekniska informationssäkerhetslösningar inom Åda, och erbjuder lösningarna till kunderna efter att de verifierats väsentliga och fungerande.
- Man har en intern informationssäkerhetsgrupp, som träffas varje vecka för att hantera informationssäkerhetsfrågor. Gruppen hanterar aktuella ärenden men jobbar även långsiktigt med policyn, riktlinjer, och kravställning för att höja mognadsnivån.
- Åda har två heltidsanställda jurister specialiserade på hantering av personuppgifters data integritet, DPO:n (Data Protection Officer). Dessa arbetar på uppdrag för kunderna.
- Åda har ytterligare en resurs som hanterar frågor kring persondata integritet (privacy), DPO internt för Åda Ab.
- Åda har också en informationssäkerhetsspecialist som är mer teknisk och arbetar på uppdrag av Åda och även med uppdrag som riktar sig mot kund.
- Servicenivån uppmäts kontinuerligt med avseenden på tillgänglighet, pålitlighet och responstider
- Mätning av ledarskap och medarbetarindex utförs kontinuerligt med en definierad process för utvärdering och hantering av utfallet
- Händelsehantering är väldefinierad och fungerar bra
- Incidenthanteringen är väldefinierad och fungerande, med kontinuerlig uppföljning
- Problemhanteringen fungerar bra och lösningarna uppföljs både internt och tillsammans med kunderna.

Sammanfattning av IT riskbedömningen

I avsnitt 3 presenteras de väsentligaste riskerna vilka identifierades på basen av kartläggningen. Som ramverk för riskbedömningen användes COSO-ERM modellen, vilken är den globala de-facto standarden för riskstyrning och intern kontroll. Kartläggningen fokuserade på risker relaterade till personer, processer samt teknologi, med en indikativ klassificering i strategiska samt operativa risker.

Sammanfattningsvis kan konstateras att,

- **riskstyrningsprocessen inom Åda Ab ligger på en informell nivå, men ansvarspersonerna inom organisationen har en god uppfattning av de centrala riskerna inom verksamheten, och riskhanteringsåtgärder har identifierats. Där som är möjligt har aktiviteter initierats för att eliminera eller åtminstone kunna mitigera (försvaga, mildra inverkan) risken**
- **ett flertal av de mest signifikanta riskerna är relaterade till omständigheter vilka ligger utanför Åda Ab:s interna kontroll.**
- **ett flertal av de mest signifikanta riskerna är grundade i Ådas oklara roll och förväntningar, och kräver en mitigering/ hantering vilken inkluderar ägarna.**

02 Nuläge, IT-verksamhet och Service Management

Avsnittet beskriver vilken övergripande **nivå av mognad** Åda bedöms besitta i nuläget inom de områden som granskats.

Nuvarande mognadsnivå

2017 (enligt uppgift Åda)

Målbild för projektet ”Skapa förutsättningar” (enligt uppgift Åda)

Nuvarande verifierad mognadsnivå. Konstaterad av KPMG

	INLEDANDE	REPETERBAR	DEFINIERAD	HANTERAD	OPTIMERAD
	Ad-hoc, oförutsägbar, dåligt kontrollerad, reaktiv	Grundläggande processhantering, repeterbara uppgifter	Definierade och dokumenterade processer, proaktiva	Processer är integrerade, uppmätta och kontrollerade	Ständig förbättring, organisatorisk anpassning
IT-styrning	• Minimal förmåga inom detta område med saknade eller informella processer och/eller beteenden. • Funktionen, tenderar att vara reaktiv i sina handlingar med brist på styrning eller kontroll.	• Viss förmåga finns, men disciplin för att genomföra processerna eller kommunicera konsekvent saknas ofta. • Det finns en förmåga att se kontroller men funktionen bygger på individens bästa avsikter och färdigheter.	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurs.	• Funktionens mål anpassas till organisationens behov. Utförandet av processerna sker i allmänhet felfritt. • Funktionen är integrerad i organisationen; proaktivt och strategiskt. • Prestanda mäts och hanteras med fokus på operativ duglighet och förutsägbara resultat. • Funktionen utvecklas och förbättras ständigt.	• Funktionen ses som exemplarisk av jämlika organisationer. • Fokus ligger på värdeutveckling med affärsrelevanta resultatmått. • Funktionen eftersträvar ständigt innovation och utmanar verksamheten samt tillför strategiskt värde med en hållbar roll i organisationen. • Funktionen tas aktivt i beaktande av resten av verksamheten för sin förmåga.
Utveckling, infrastruktur					
Drift					
Planering och projektstyrning					
Informations-säkerhet					
Service Management					

Ådas mognadsnivå

Att beakta då man tolkar maturitetsanalysen:

- Ådas mognad har granskats i förhållande till den kravställning som för tillfället ställs på Åda. Ur detta perspektiv är Åda på en relativt hög mognadsnivå och klarar av att leverera till sina kunder klart över den förväntade nivån.
- Mognadsnivån är jämförbar med motsvarande driftsleverantörer som fungerar geografiskt inom samma område med samma kravställning.
- Åda skulle ha kapacitet och förutsättningar att inom alla delområden nå en proaktiv och målstyrd nivå med mera långsiktiga och enade beställare
- En högre mognadsnivå sänker typiskt omkostnaderna genom ännu effektivare investeringar, processer, kravställningar och specifikationer enligt standardenliga mallar.

Delområde	Maturitetsnivå	Förklaring	Trend
IT-styrning	3 - DEFINIERAD Definierade och dokumenterade processer, proaktiva	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurs.	Man har klart nått en mognad som överensstämmer med behovet just nu. Det finns egentligen ingen beställning på en högre mognad, även om man genom ytterligare effektivisering och automatisering av processerna skulle komma till högre kostnadseffektivitet och kvalitet. I praktiken fungerar IT-styrningen enligt behoven bra.
Utveckling, infrastruktur	2 - REPETERBAR Grundläggande processhantering, repeterbara uppgifter	• Viss förmåga finns, men disciplin för att genomföra processerna eller kommunicera konsekvent saknas ofta. • Det finns en förmåga att se kontroller men funktionen bygger på individens bästa avsikter och färdigheter.	Mognaden inom utveckling kunde relativt enkelt höjas till nivå 3, genom skapandet av referensarkitektur och standardiserade lösningar. Vårt antagande är dock, att genom Åda Hosting, kommer även maturiteten på utveckling att höjas.
Drift	3 - DEFINIERAD Definierade och dokumenterade processer, proaktiva	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurs.	Man har klart nått en mognad som överensstämmer med behovet just nu. Det finns egentligen ingen beställning på en högre mognad, även om man genom ytterligare effektivisering och automatisering av processerna skulle komma till högre kostnadseffektivitet och kvalitet. I praktiken fungerar driften enligt behoven bra
Planering och projektstyrning	4- HANTERAD Processer är integrerade, uppmätta och kontrollerade	• Funktionens mål anpassas till organisationens behov. Utförandet av processerna sker i allmänhet felfritt. • Funktionen är integrerad i organisationen; proaktivt och strategiskt. • Prestanda mäts och hanteras med fokus på operativ duglighet och förutsägbara resultat. • Funktionen utvecklas och förbättras ständigt.	Man är klart på en mognad som överträffar behovet just nu. Detta är dock ett viktigt område, där en högre mognad lätt resulterar i bättre kostnadseffektivitet, kvalitet och kundnöjdhet. Vi anser det viktigt att upprätthålla denna nivå och samtidigt kontinuerligt utveckla och förbättra funktionen.
Informations-säkerhet	2 - REPETERBAR Grundläggande processhantering, repeterbara uppgifter	• Viss förmåga finns, men disciplin för att genomföra processerna eller kommunicera konsekvent saknas ofta. • Det finns en förmåga att se kontroller men funktionen bygger på individens bästa avsikter och färdigheter.	Mognaden överensstämmer med behovet just nu, men här bör Åda fungera som vägledare mot sina kunder och öka mognaden. Detta är redan under arbete, och vi ser att en allt högre mognad är möjlig genom det arbete som nu har satts igång.
Service Management	3 - DEFINIERAD Definierade och dokumenterade processer, proaktiva	• Funktionens tillstånd är tillförlitligt och processer implementeras, vilket leder till ett konsekvent tillvägagångssätt men med brist på integration till andra funktioner. • Det finns etablerad styrning, mätning och kontroll. • Funktionen tillhandahåller definierad kompetens och resurs.	Man är klart på en mognad som överträffar behovet just nu. Detta är dock ett viktigt område, där en högre mognad lätt resulterar i bättre kostnadseffektivitet, kvalitet och kundnöjdhet. Vi anser det viktigt att upprätthålla denna nivå och samtidigt kontinuerligt utveckla och förbättra funktionen och eventuellt öka mognaden till nivå 4 i fortsättningen.

03 IT riskanalys

Avsnittet beskriver **hur** IT riskanalysen utförts, **vilka risker som identifierats** samt vilken **nivå** riskerna har.

Metod för IT riskanalys

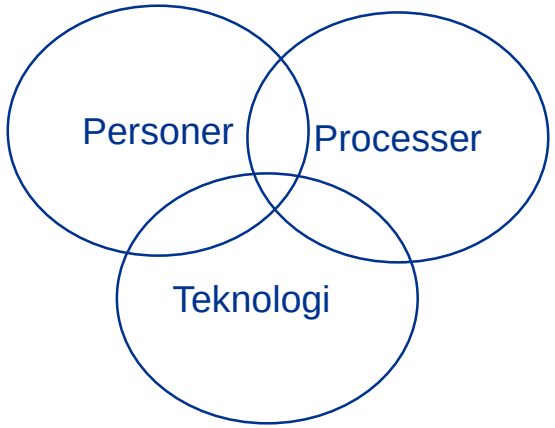
Som ramverk för riskbedömningen användes COSO-ERM modellen, vilken är en internationell, allmänt accepterad modell för riskstyrning och intern kontroll. Vi fokuserade på risker relaterade till personer, processer samt teknologi, med en indikativ klassificering i Strategiska samt operativa risker.

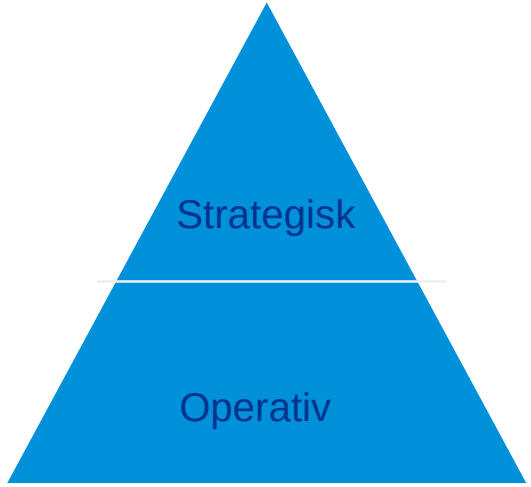
COSO-ERM

En internationell, allmänt accepterad modell för intern kontroll

- ***Intern miljö***
- ***Målformulering***
- ***Händelseidentifiering***
- ***Riskbedömning***
- ***Riskåtgärder***
- ***Kontrollaktiviteter***
- ***Information/ kommunikation***
- ***Övervakning inkl. uppföljning/ utvärdering***

Source: COSO ERM - The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Framework 2003.

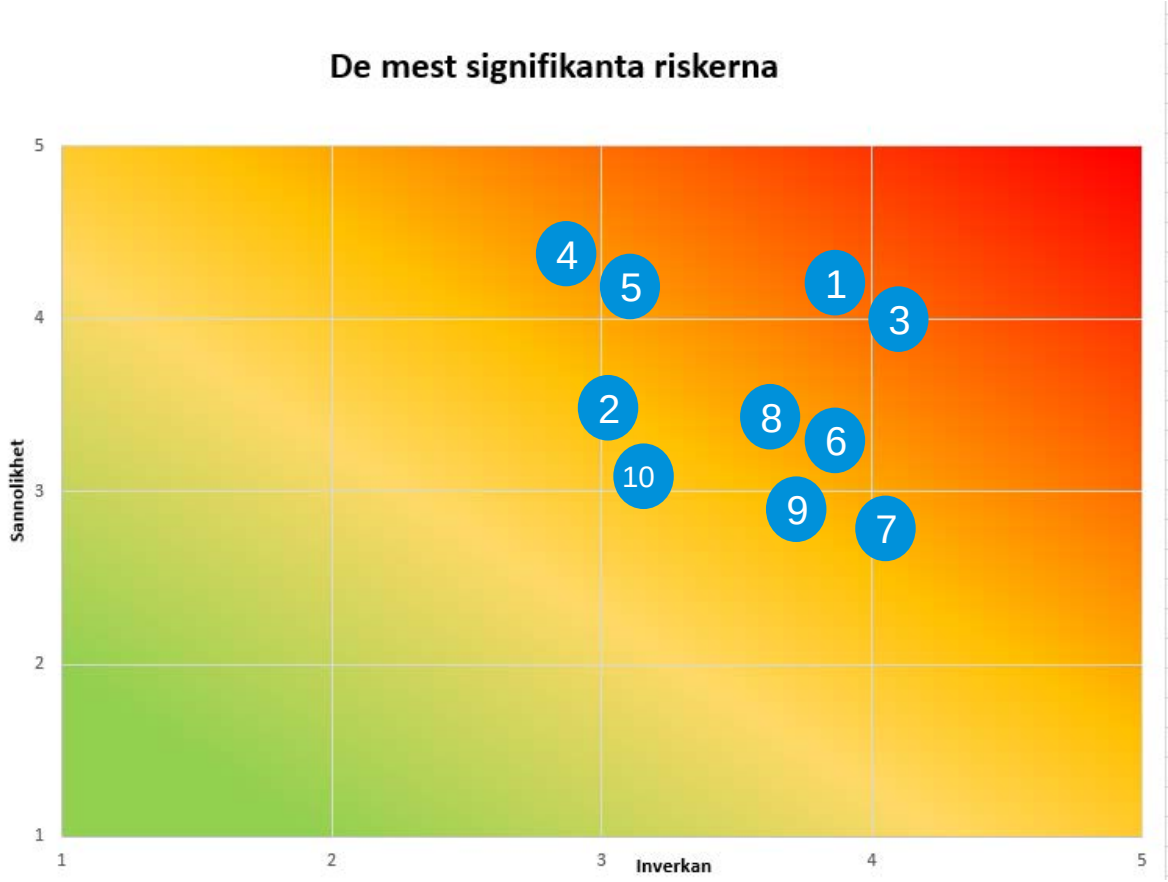




Riskregister

Nedan presenteras en aggregerad sammanställning av identifierade risker samt en riskkarta. De identifierade riskerna är inte rangordnade.

Ref	Identifierad risk
1	Otydlig ägarstyrning och målbild
2	Negativ publicitet
3	Otydliga krav på Informationssäkerhet och säkerhetsklassning
4	Personberoende (nyckelpersoner, kompetenser)
5	Svårighet att rekrytera specialister
6	Låg beställarkompetens
7	Oenhetlig IT arkitektur
8	Föråldrad och/eller oenhetlig teknologi
9	Tjänstehantering i en icke-standardiserad driftsmiljö
10	Otydlighet i beställare- ägare processer och roller



04 Föreslagna Åtgärder

Avsnittet definierar Ådas **styrkor** och **utmaningar** samt ett antal **konkreta åtgärder** per analyserat område samt ger en kortfattat **beskrivning till varför** dessa åtgärder är nödvändiga.

IT-styrningen fungerar i sin helhet bra och mognaden motsvarar behovet

IT-styrning

Utveckling, infrastruktur

Drift

Planering och projektstyrning

Informations-säkerhet

Service Management

Mognadsnivå för delområdet: *Mognadsnivå 3*

Styrkor

- Åda har en strategi som löpande sträcker sig tre år framåt (fastställd av styrelsen)
- Åda har en verksamhetsplan för ett år i taget med mål och KPI:er
- Åda strävar efter att själv i främsta hand använda sig av beprövad teknologi som ständigt evalueras och därmed ger Åda själv insikt i hur det skulle fungera hos kunden.
- Budgetmålen baserar sig på en kombination av tidigare konsumtion och prognoser
- Åda har en tydlig uppdelning av ansvar, ledning och beslutsfattning
- Man styr resurser till att fokusera aktiviteter på att uppnå intressenternas prestationsförväntningar och mål

Utmaningar

- Långsiktig planering av projektintäkter (50% av Ådas intäkter) är svårt att estimera, då kunderna och Åda själv fungerar ett budgetår i taget.
- Kravställningen blir utmanande då kunderna och ägarna är de samma, man känner att man inte kan ställa krav på sina ägare.
- Ägarna ser Åda mest som en operativ enhet och skulle gärna undvika kostnaderna för strategisk ledning och administrativa åtgärder som hör till en tjänsteleverantör. Till detta hör t.ex. licenshantering, livscykelhantering och också riskhantering, som sätter sin prägel i mognaden i att evaluera och hantera IT risker

Åtgärder

1

Det är utmanande med långsiktig planering då ägarnas styrning ger vägledning endast ett budgetår i taget, vilket leder till att det också är svårt att estimera intäkter längre än ett år i taget. Detta leder till utmaningar i att göra effektiva mer långsiktiga investeringsbeslut.
En förbättring för Ådas del skulle vara att regeringen respektive ägarna fastslår en konkret och långsiktig digital strategi för den offentliga sektorn, samt en för ägarna gemensam långsiktig målbild där det klart beskrivs vad som förväntas av Åda de inkommande 3-5 åren. Strategin skall ha en möjlighet att överleva ändringar i den politiska miljön.

2

Ett grundläggande problem är det unika kund-/ägo förhållandet, men detta får inte ses som ett hinder för att kräva t.ex. kvalificerad kravställning för upphandling, klara krav på informationssäkerhet samt tydlig styrning mot samordning, gemensamma tjänster och enhetliga processer.

I avsaknad av en aktiv strategisk beställare förslås att Åda får i uppdrag av ägarna att leda, genom att för sin egen driftsmiljö ta fram

- En målbild för en enhetlig arkitektur
- Standarder för tekniska lösningar i enlighet med målbilden för Ådas arkitektur
- En transparent livscykel- och licenshantering
- Samt åtgärder som återfinns under rubriken informationssäkerhet

Utveckling, infrastruktur kunde genom små åtgärder höja sin mognad

Mognadsnivå för delområdet: *Mognadsnivå 2*

Styrkor

— Åda har en välstrukturerad modell för planering och projektstyrning, vilken också används vid utveckling av infrastruktur

Åtgärder

Utmaningar

— Man har ingen dokumenterad referensarkitektur eller målbild för IT miljön, vilket gör att även om man vill styra kunderna mot mera standardenlig och uniform miljö, har man ingen dokumentation som stöder detta.
— Kunderna ser inte alltid behovet/nyttan av att göra kravställning, vilket gör att Åda måste ägna mycket av sin tid att göra kravställning och antaganden för kundens räkning.
— Bristen på kravställningskompetens hos kunden återspeglar sig ofta på Åda på ett negativt sätt, speciellt om ett projekt inte lyckas på grund av vag kravställning.
— Det är en stor variation mellan kundernas kompetens inom kravställning och upphandling, vilket resulterar i mycket varierande lösningar som upphandlas.

1. En målbild och referensarkitektur för IT-miljön borde skapas, för att man bättre skall kunna styra kunderna mot en mera standardenlig och uniform IT-miljö.
2. Som helhet borde Åda bli mera krävande mot sina kunder och sätta upp kravställning med sina kunder över miljön de driver. Problemet är i stort det unika kund-/ägoförhållandet, men detta får inte ses som ett hinder till att kräva t.ex. kvalificerad kravställning för upphandling, klara krav på informationssäkerhet samt tydlig styrning mot samordning, gemensamma tjänster och enhetliga processer.

Driften fungerar i sin helhet bra och mognaden motsvarar behovet

- IT-styrning
- Utveckling, infrastruktur
- **Drift**
- Planering och projektstyrning
- Informations-säkerhet
- Service Management

Mognadsnivå för delområdet: *Mognadsnivå 3*

Styrkor

- Åda har en väl fungerande process för upphandling av informationsteknisk utrustning, baserat på ett ramavtal.
- Ovannämnda process innefattar även snabb småskalig utveckling, som inte kräver projekt för att genomföras. Större förändringar genomförs alltid via projekthanteringsprocessen.
- Man har förutsättningar att leverera mot SLA, trots att alla kunder inte ens kräver SLA (Serice level agreements)
- Driften baserar sig på standardiserade processer, vilket gör det lättare för Åda att jobba mot tredje part, t.ex. Ådas egna eller kundens leverantörer.

Utmaningar

- Då man driftar bas IT som man inte äger, går man miste om alla de skalfördelar samordning av IT-verksamheten tillför:
  - Enhetlig arkitektur
  - Standardenlighet
  - Upprätthållandet av rätt expertis
  - Livscykel- och licenshantering
- Nuvarande modell där kunderna äger sin bas IT ger inte tillräckligt underlag för att utveckla gemensamma tjänster för offentliga förvaltningen, vilket medför ökade kostnader både på kort och på lång sikt.

Åtgärder

1. Mandat och ansvar för standardisering är av stor betydelse för att nå skalfördelar av samordningen. Åda borde kunna äga de tekniska besluten och ramverken för bas IT:n, så att Åda kan standardisera den tekniska miljön och tillämpa livscykelhantering, kostnadseffektiva, gemensamma informationstekniska lösningar och tjänster. Åda kan fungera som drivande kraft, men kravet bör komma från Landskapsregeringen.

2. För en säker och ändå flexibel it-drift behöver man skapa ramar för vad som är tillåtet och hur man hanterar risker i it-miljön. Ägarna bör stötta Ådas framtagning av:
   - En målbild för en enhetlig arkitektur
   - Standarder för tekniska lösningar i enlighet med målbilden för Ådas arkitektur
   - En transparent livscykel- och licenshantering

3. Åda bör i den utsträckning det är möjligt, skapa gemensamma tjänster för offentliga sektorn som t.ex.
   - Centraliserad logghantering
   - Centraliserad identitetshantering
   - Centraliserad integrationsplattform
   - Teknisk monitorering

4. Som del av livscykelhanteringen, bör Åda målmedvetet driva in sina egna prefererade arkitekturer och standarder vid upphandling av nya system

Planering och projektstyrning överträffar behovet i sin mognad

Mognadsnivå för delområdet: *Mognadsnivå 4*

Styrkor

- Planeringen av Ådas verksamhet baserar sig på styrelsens strategi, som bryts ner till verksamhetsplan, som i sin tur tar i beaktande kundernas behov i form av vägkarta. I sin helhet fungerar detta bra, men i teorin inte långsiktigt (se utmaningen nedan).
- Man har modeller för prioritering både av kundaktiviteter och interna aktiviteter för ett budgetår i taget.
- Man startar projekt med förstudie, på basen av vilket ett utvecklingsprojekt antingen startar eller förkastas. Detta är en bra kutym och minskar risken för misslyckande.
- Projektstyrningen överlag på en god nivå med tydliga steg och klara roller både hos Åda och kunden.
- Man försöker aktivt föra över Ådas strukturella sätt att jobba till sina kunder.

Utmaningar

- Den överliggande strategin för digitalisering av den offentliga förvaltningen saknas. Riktlinjerna som dras ändrar också periodvis via politiska beslut. Detta är den stora skillnaden mot fastlandet, där samma digitala strategi, och nu också digital cyber strategi slås fast och utarbetas i samma riktning oberoende av politisk påtryckning. Riskerna relaterade till kontinuitet har en stor negativ effekt på Åda:s utveckling.
- Det finns en stor personrisk på Åda, eftersom det är svårt att rekrytera tekniskt kunniga personer för tillfället på Åland. Detta medför utmaningar för mera långsiktig planering.

Åtgärder

1. För att möjliggöra för Åda att skapa en egen långsiktig målbild, bör det finnas en fastslagen, långsiktig digital strategi för den offentliga sektorn, där det klart beskrivs vad som förväntas av Åda de inkommande 3-5 åren. Strategin skall ha en möjlighet att överleva förändringar i den politiska miljön.
2. Åda kan bättre möta kundens förväntningar om ägarna utvecklade sin mognadsnivå som beställare och förvaltare av sina IT-investeringar.
3. Åda strävar till att upprätthålla en generaliserad IT kompetens hos sig själv, och köpa in specialkompetens via ramavtal. Detta är strategiskt vettigt för att minimera personrisken man för tillfället har.

Informationssäkerhetens mognadsnivå utvecklas konsekvent

- IT-styrning
- Utveckling, infrastruktur
- Drift
- Planering och projektstyrning
- **Informations-säkerhet**
- Service Management

Mognadsnivå för delområdet: *Mognadsnivå 2*

Styrkor

- Man testar aktivt nya tekniska informationssäkerhetslösningar inom Åda, och erbjuder lösningarna till kunderna efter att de verifierats väsentliga.
- Man har börjat med återkommande tekniska penetrationstester för att kontrollera hur olika tekniska informationssäkerhetskontroller fungerar.
- Man har en intern informationssäkerhetsgrupp, som träffas varje vecka för att hantera informationssäkerhetsfrågor. Gruppen hanterar aktuella ärenden men jobbar även långsiktigt med policyn, riktlinjer, och kravställning för att höja mognadsnivån.
- Man har två heltidsanställda DPO:n (Data Protection Officer) som hanterar frågor kring privacy både internt för Åda, men också för Ådas kunder. Personerna bjuds in i säkerhetsgruppen vid behov.

Utmaningar

- Åda har under de tre senaste åren gjort en kraftansträngning för att höja mognaden på informationssäkerheten. Mognaden på hela Åland vad beträffar informationssäkerhet har länge varit tämligen låg, så det är fråga om en stor kulturändring i förhållningen till ämnet.
- Den interna informationssäkerhetsguppen har ett väldigt stort ansvar i utvecklandet av informationssäkerheten, men man har inget egentligt mandat för beslut eller budgetansvar över informationssäkerhetslösningar.
- Kunderna ställer normalt inga karv på informationssäkerhet och de klassificerar normalt inte sin informationen som hanteras i de system som hostas (administreras) i Ådas miljö. Det är svårt att uppnå kostnadseffektivitet med tanke på teknisk informationssäkerhet, då man inte vet hurudan skyddsnivå är tillräcklig för olika system.
- Den fysiska säkerheten på kontrosnivå (Åda, iTiden) är relativt svag, då man t.ex. saknar kameraövervakning.

Åtgärder

1. Det finns få instanser som ställer krav mot Åda eller Ådas kunder på mognaden av informationssäkerheten. Det är en stark rekommendation att Landskapsregeringen utvecklar en gemensam kravställning, eller att Landskapsregeringen ger mandat åt Åda att skapa en gemensam kravställning som kunderna implementerar, för alla instanser inom förvaltningen. Detta är det enda sättet att skapa förutsättningar för en informationssäker digitalisering av Åland.
2. Utöver kundens ansvar som informationsägare kan Ådas interna säkerhetsgrupp utgöra ett viktigt komplement. Ådas interna säkerhetsgrupp är ytterst viktig för att uppnå en högre maturitet inom informationssäkerheten. Det är viktigt att utveckla denna resurs vidare så, att gruppen både har ett mandat att ta beslut, samt ett budgetansvar för aktiviteter inom utvecklandet av informationssäkerheten.
   Ägarna skulle också ha stor nytta av att Ådas interna säkerhetsgrupp samarbetar med säkerhetsgruppen som polisen och räddningsväsendet har gemensamt, eftersom det finns mycket gemensamma intressen mellan dessa tre parter inom utvecklandet av informationssäkerheten.
3. Man har en dedikerad informationssäkerhetsexpert som jobbar en dag i veckan. Med tanke på innestående jobb att förhöja mognaden på informationssäkerheten, rekommenderas en heltidsanställd ansvarsperson.
4. Åda kan bättre möta kundens förväntningar om ägarna själva förbättrade sin mognadsnivå som informationsägare och förvaltare av sin information.
   Ägarna bör leda med sin egen informationssäkerhetspolicy och dokumenterad klassning av information och därmed systemens krav på skyddsnivå.
   Åda kan fungera som drivande kraft, men policy och klassning kommer från kunden.
5. Åda bör höja nivån på den fysiska säkerheten i sitt kontor genom säkerhetsanordningar så som slutna utrymmen för gäster, slutna utrymmen för arbete med sensitiv data och kameraövervakning.

Tjänstehanteringen fungerar i sin helhet bra och mognaden motsvarar behovet

- IT-styrning
- Utveckling, infrastruktur
- Drift
- Planering och projektstyrning
- Informations-säkerhet
- Service Management

Mognadsnivå för delområdet: *Mognadsnivå 3*

Styrkor

- Service katalogen är utarbetad tillsammans med kunderna.
- Service Level Agreement (SLA) och Operational-Level Agreement (OLA) överses kontinuerligt, samt dess efterlevnad genomgås kontinuerligt med kunderna.
- SLA samt tjänsterna uppmäts kontinuerligt för tillgänglighet, pålitlighet och responstider.
- Händelsehantering i sin i sin helhet är väldefinierad och fungerar bra
- Incidenthanteringen är väldefinierad och fungerande, med kontinuerlig uppföljning
- Problemhanteringen fungerar bra och lösningarna uppföljs både internt och tillsammans med kunderna.

Utmaningar

- Efterlevnad av SLA och OLA i en driftsmiljö som inte är standardiserad är utmanande och arbets-drygt och inkluderar i värsta fall också samordnade komponenter (ex. AD) vars SLA och OLA kan avvika
- Ändringar (Change) och åtgärdade problemlösningar (Incident management) uppföljs inte konsekvent med kunderna
- Man mäter inte utförda ändringar mot ursprunglig kravställning, vilket skulle ge mervärde åt både Åda och kunden.
- ITIL UC (underleveranshantering) utförs inte enligt process, varken under SLA eller OLA.
- Fredningstiderna planeras inte proaktivt tillsammans med kunderna.

Åtgärder

1. En enhetlig arkitektur och standardiserade lösningar skulle avsevärt underlätta definition och efterlevnad av SLA och OLA. Åda borde, som nämnts i kapitlet för drift, skapa en arkitekturbeskrivning och standardisering av miljön, vilken kunderna förbinder sig till.
2. Införandet av bättre rapportering och statistik kring tjänsterna och processerna (t.ex. antalet hanterade problem och incidenter, tjänsternas up-time, kostnadseffektivitet), skulle ge en mera transparent och rättvisande bild av Ådas service management processer.
3. Implementeringen av ITIL:s UC processer (underleveranshantering) i Service Management processhelheten skulle minska risken att det inskaffas samma tjänster åt olika kunder på olika sätt med olika avtal
4. Förbättra kommunikationen kring fredningstiderna på lång sikt för att undvika onödiga kostnader och missnöje hos kunden

05 Appendix

Intervjuade personer

Åda

- Katarina Donning - vd
- Lynn Häggblom - projektchef
- Anette Korpi – Administrativ chef
- Christer Lindblom – change manager
- Marina Ekqvist – operativ it-chef
- Camilla Sundkvist - processägare
- Monica von Frenckell – processledare problem/teamledare
- Jonas Grönholm – processledare incident
- Jeanette Viktorsson – HR- administratör
- Sven Sjöblom (tekniker/driftsansvarig)
- Robin Hjerpe (tekniker(teamledare)
- Fredrik Pettersson(tekniker/teamledare)
- Virginia Horniak (extern konsult) – informationssäkerhetsexpert

Landskapsregeringen som kund och beställare

- Ronny Lundström – Förvaltningsansvarig it

Analyserad dokumentation

KPMG har som en del av sin granskning tagit del av följande sekretessbelagda dokument

- **Åda KPI 1.0 2020.xlsx**
- **Ansvarsfördelning Åda_lagtinget_20200828.xlsx**
- **Förteckning policy, instruktioner för Åda Ab_20200130.xlsx**
- **iSeries Skakrav.pdf**
- **LG-rapport 2020 Augusti.pptx**
- **Mål 2020 ALLA.xlsx**
- **Projektprioriteringsmodell.pptx**
- **Stuart Skakrav.pdf**
- **Slutrapport Gemensam övervakning.docx**
- **Översikt Åda Jourberedskap.docx**
- **Åda informationssaäkerhet Maj 2021.docx**
- **Åda_informationssäkerhetspolicy_1.0 - fastställd av styrelsen 27.2.2020.docx**
- **UTKAST Åda riktlinjer inom informationssäkerhet-kommentarer BORTTAGNA.docx**
- **HR-processen-202006.pptx**
- **Mandat&ansvar inom Åda Ab-övergripande&inköp-20190901.pdf**
- **SFIA kompetenskartläggning_sammanfattning för Åda Ab 20200130.pptx**
- **SFIA_kartlaggning_Ada_v1.0_ 2019.xlsx**
- **Utbildningsplan_2020 (1).xlsx**
- **2019-01-16 Service request processen.pdf**
- **2020-06-24 Normal Change process.pdf**
- **Arbetssätt på Åda.pptx**
- **Huvudprocess.vsdx**
- **Modell för förstudie och upphandlingsfas.pdf**
- **Projektprocess frÃ¥n bestÃ¤llning till avslutat projekt.png**
- **Publik Major Change.pdf**
- **Projektplan_Åda.pdf**
- **MALL - Förvaltningsplan v1.3.docx**
- **MALL_Tjänstebeskrivning_tjänst.docx**
- **Prioriterade_förslag_ITtjänst_mall v1.0.xlsx**
- **Rollbeskrivning tjänstesamordnare v1.0.docx**
- **Rollbeskrivning tjänsteägare v1.0.docx**
- **SLA för tjänstebeskrivning ver 1.0.pdf**
- **Tjänstebeskrivning Datacenter_Drift v1.0 (2).pdf**
- **Tjänstebeskrivning Support v1.0 (1).pdf**
- **Tjänsteförvaltningsmodellen v1.5.pptx**