Protokollsbilaga C5
Direktionens protokoll 2022-12-19, §5

Beslutsunderlag

DATUM: 2022-12-19
AVDELNING: Avdelningen för IT- och Digitalisering
HANDLÄGGARE: Ulrika Pilestål
HANTERINGSKLASS Ö P P E N

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2022-01073

Beslutsunderlag – uppdaterad IT- och digitaliseringspolicy

Förslag till direktionens beslut

Direktionen beslutar att Riksbankens IT- och digitaliseringspolicy ska uppdateras och att den nya policyn träder i kraft samma dag. Genom detta beslut upphävs tidigare IT- och digitaliseringspolicy från 2021-06-07 med diarienummer 2021–00634. Beslut fattas även om att godkänna IT- och digitaliseringsstrategin som uppdaterats med hänsyn till etablering av avdelningen för IT och digitalisering (AID) som egen avdelning samt anpassning för den nya regeln om väsentlig verksamhetsförändring.

Ärendet

Ärendet avser årlig uppdatering av ”IT- och digitaliseringspolicy” samt anpassning till ny mall för styrande dokument samt justering av IT- och digitaliseringsstrategin.

Överväganden

Riksbankens IT- och digitaliseringspolicy har genomgått en årlig översyn och uppdatering i enlighet med Regel för Riksbankens styrande dokument. Policyn har anpassats till Riksbankens nya mall för styrande dokument vilket innebär att dokumentet har kompletterats med nödvändig information för att uppfylla kraven i den nya mallen. Synpunkter har inhämtats från RÄT, klarspråk och regelefterlevnadsspecialist och omhändertagits vid uppdatering av denna policy.

Riksbankens IT- och digitaliseringsstrategi har uppdaterats med hänsyn till etablering av avdelningen för IT och digitalisering som egen avdelning samt anpassning för den nya regeln om väsentlig verksamhetsförändring. Ändringarna är markerade i dokumentet.

Föreslagen policy innebär inte några förändringar av innebörd eller sakinnehåll. Uppdateringar som gjorts syftar till att göra policyn tydligare och enklare att ta till sig för alla medarbetare på Riksbanken. Uppdateringar inkluderar även vissa anpassningar för att omhänderta förändringar exempelvis etableringen av AID som egen avdelning.

IT- OCH DIGITALISERINGSPOLICY

BESLUTSDATUM:	2022-12-19
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	Avdelningen för IT och digitalisering
FÖRVALTNINGSANSVARIG:	Ulrika Pilestål
DIARIENUMMER:	2022-01073
HANTERINGSKLASS:	ÖPPEN

IT- och digitaliseringspolicy

Innehåll och syfte

Denna IT- och digitaliseringspolicy syftar till att tydliggöra hur vi ska arbeta med IT och digitalisering för att Riksbanken ska uppnå sina strategiska och taktiska mål. Den syftar också till att säkerställa att Riksbankens investeringar och aktiviteter inom IT och digitalisering utgår från Riksbankens strategier och verksamhetens behov samt att IT-organisationen arbetar proaktivt och nära verksamheten på ett resurseffektivt sätt. Principerna i denna policy ska gälla i IT- och digitaliseringsarbetets hela process, från planering till implementation, livscykelhantering och utfasning.

Målgrupp

Denna policy riktar sig till Riksbankens samtliga medarbetare, inklusive leverantörer av IT-tjänster och konsulter, och framförallt till de som är beroende av IT, digitalisering och stabil IT-drift för utveckling av sin verksamhet.

Innehållsförteckning

1 Inledning

IT-verksamheten ska bidra till att Riksbanken verkar på medborgarnas uppdrag för en stark och säker ekonomi samt uppnår visionen *att vara en nytänkande centralbank med hög beredskap och en utvecklande arbetsplats.*

1.1 Bakomliggande regelverk

Huvudsakligen dataskyddsförordningen och säkerhetsskyddslagen.

1.2 Definitioner

IT-verksamheten avser alla IT-aktiviteter som utförs inom Riksbanken.

IT-organisationen avser organisationen avdelningen för IT och digitalisering

Cybersäkerhet avser tekniska och administrativa åtgärder för skydd mot fientliga eller illvilliga, externa IT-hot.

Security Operations Center (SOC) bidrar till att skydda Riksbanken mot IT- och cyberhot samt vidareutveckla Riksbankens IT- och cyberskydd och förmågor. Arbetet sker utifrån informationens klassificering och verksamhetens krav och riskbedömning.

2 Roller och ansvar

Riksbankens avdelningschefer ansvarar för att den verksamhet som bedrivs sker i enlighet med denna policy. Detta gäller oavsett i vilken regi detta sker, och oavsett om hela eller delar av verksamheten utförs av en extern utförare.

Riksbankens IT-chef, tillika chefen för avdelningen för IT och digitalisering (AID), säkerställer att policyn överensstämmer med de regler som finns inom området och ansvarar för att förvalta policyn och informera om innehållet i den. IT-chefen ansvarar för att avdelningen för IT- och digitalisering har den kompetens och de resurser som krävs för att Riksbankens verksamhet ska kunna agera i enlighet med IT- och digitaliseringsstrategin och denna policy.

3 Styrande principer för IT-verksamheten

Denna policy utgår ifrån och stödjer Riksbankens strategiska plan med fokus på nytänkande och hög beredskap;

• *Nytänkande* – i vårt tjänsteutbud, genom digitalisering och innovation samt i vår kommunikation

I våra verksamheter och på betalningsområdet måste vi tänka nytt och anpassa vårt tjänsteutbud och arbetssätt till hur vår omvärld förändras. Vi ska använda de möjligheter som ny teknik och ny information ger.

• *Hög beredskap* – operationellt, finansiellt och i vår analys

En utmaning för att nå hög beredskap är att upprätthålla en hög säkerhet och beredskap (inkl. cybersäkerhet) för våra kritiska system. Vår analys behöver vila på en robust grund, baseras på forskning och ligga i framkant med hög beredskap att snabbt svara upp mot nya utmaningar.

IT-verksamheten ska bedrivas i enlighet med beslutad IT-och digitaliseringsstrategi och därmed utveckla följande områden:

- säkra stabil drift och förvaltning
- cybersäkerhet och SOC
- effektiva arbetsformer
- stöd och verktyg för dataanalys
- IT-arkitektur och strukturkapital
- stöd i verksamhetsutveckling
- digitalisering och innovation

Styrande principer

Följande **styrande principer** ska gälla för IT-verksamheten:

- Avdelningen för IT- och digitalisering ska driva Riksbankens digitala utveckling och samtidigt leverera en robust och säker förvaltning av hög kvalitet.
- IT-satsningar ska utgå från verksamhetens behov och i första hand ska färdiga tjänster, funktioner eller IT-stöd köpas in. Egenutveckling ska endast ske för Riksbanksspecifika behov där väsentlig nytta kan påvisas eller en passande lösning inte finns att köpa.
- IT-organisationen ska vara nytänkande och drivande i att skapa förutsättningar för Riksbanken att testa nya lösningar i en stimulerande och innovativ miljö.
- IT-organisationen ska ha en helhetsbild över bankens alla IT-kostnader. Förvaltningen av IT-stödet ska utgå från verksamhetens processer.
- IT-säkerhetsnivån ska vara hög och anpassad till behoven inom olika områden samt utgå från de hanteringsklasser som gäller för Riksbankens information.
- IT-arkitekturen ska baseras på välkända och standardiserade lösningar samt vara styrande vid förändringar i IT-miljön. Nya lösningar kan prövas inom områden där säkerhetskraven så medger och där det finns ett behov av snabbare utveckling, till exempel IT-arbetsplats och analysområdet. Användning av molntjänster ska alltid beaktas vid ny- och vidareutveckling.
- IT-organisationen ska ha egen kompetens inom strategiska verksamhetsområden för både IT och Riksbanken. Utkontraktering ska

ske av IT-verksamhet som inte är specifik för Riksbanken och där det finns en extern part som kan utföra verksamheten enligt Riksbankens krav och övergripande mål.
- Beslutade styrmodeller och arbetsprocesser ska användas för att leverera IT-tjänster effektivt och med tillräcklig kvalitet.

Kompetens och stöd inom Riksbanken

För att Riksbanken ska få ett stabilt, säkert och tillgängligt IT-stöd ska avdelningen för IT- och digitalisering ha kompetens för att kunna leverera inom följande tjänsteområden:

- stöd i verksamhetsutveckling och förändringsarbete
- digitalisering, innovation och nya teknologier
- IT-arkitektur och strukturkapital
- projektledning, metodstöd och kvalitetssäkring
- förvaltning av Riksbankens IT-stöd
- leverantörsstyrning och leveransuppföljning
- IT-drift och support
- IT-säkerhet och SOC
- internationellt IT-samarbete.

4 Efterlevnad

Avdelningschefen för avdelningen för IT och digitalisering gör årligen en kontroll av att policyn efterlevs och rapporterar detta till direktionen i avdelningens tertialrapportering för tertial 1.

5 Ikraftträdande och övergångsbestämmelser

Denna regel träder i kraft 2022-12-19 och ersätter då tidigare beslutade Policy för IT- och digitalisering med diarienummer 2021–00634.

5.1 Versionshistorik

Senast granskad	Version	Kommentar till ändringar
2022-10-05	1.0	Anpassning till Riksbankens nya mall för styrande dokument samt till Regel för Riksbankens styrande dokument.

Checklista

Syftet med denna checklista är att dokumentera kvalitetsgranskning av en policy eller regel. Checklistan ska fyllas i av förvaltningsansvarig.

Checklistan ska bifogas beslutsunderlaget till beslutsfattare.

Namn på styrande dokument: IT- och digitaliseringspolicy

Datum för kvalitetsgranskning: 2022-11-22

Namn på förvaltningsansvarig: Ulrika Pilestål

Aktivitet	Genomfört	Ej tillämpligt
Dokumentet är skrivet enligt befintlig mall	X	
Dokumentet är avstämt mot andra styrande dokument	X	
Dokumentet har blivit språkgranskat (av Kommunikationsenhetens klarspråksansvarige om dokumentet beslutas av direktionen)	X	
Dokumentet har granskats av RÄT	X	
En införandeplan är framtagen		X
En kommunikationsplan är framtagen		X
En utbildningsplan är framtagen		X
Det finns ett beslut om översättning till engelska, när så behövs		X
Dokumentet är granskat av Regelefterlevnadsfunktionen	X	
Checklistan har stämts av med regelefterlevnadsfunktionen	X	

BESLUTSDATUM:	2022-12-19
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	Avdelningen för IT och digitalisering
FÖRVALTNINGSANSVARIG:	Ulrika Pilestål
DIARIENUMMER:	2022-01304
HANTERINGSKLASS:	Ö P P E N

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

IT- och digitaliseringsstrategi för Riksbanken 2021-2023

Innehåll

1 Sammanfattning

Syfte med detta dokument är att beskriva på vilket sätt IT-verksamheten[1] ska bidra till att Riksbanken uppfyller sina mål. Målgruppen för dokumentet är alla medarbetare på Riksbanken.

Utvecklingen går fort och drivkrafterna är många, t.ex. pandemin som har skapat stora förändringar i sättet att arbeta. Även kombinationen av sociala medier, molntjänster, mängden tillgänglig data och mobilitet har bidragit till att ytterligare öka möjligheterna och förändringstakten med hjälp av IT samtidigt som utmaningarna med att upprätthålla en tillfredställande IT-säkerhet blir allt större.

Syftet med IT-verksamheten är att bidra till att Riksbanken verkar på medborgarnas uppdrag för en stark och säker ekonomi samt uppnår visionen *att vara en nytänkande centralbank med hög beredskap och en utvecklande arbetsplats.*

- *Nytänkande – i vårt tjänsteutbud, genom digitalisering/innovation och i vår kommunikation:* I våra verksamheter och på betalningsområdet, måste vi tänka nytt och anpassa vårt tjänsteutbud och arbetssätt till hur vår omvärld förändras. Vi ska använda de möjligheter ny teknik och ny information ger.

- *Hög beredskap – operationellt, finansiellt och i vår analys:* En utmaning för att nå hög beredskap är att upprätthålla en hög säkerhet och beredskap (inkl. cybersäkerhet) för våra kritiska system. Vår analys behöver vila på en robust grund, baseras på forskning och ligga i framkant med hög beredskap att snabbt svara upp mot nya utmaningar.

En stabil och säker drift och förvaltning är IT-verksamhetens kärnleverans och högsta prioritet. Därutöver är flertalet initiativ i den strategiska planen beroende av IT-utveckling. För att bidra till att utveckla Riksbanken i enlighet med strategin ska IT prioritera och utveckla följande områden under tidsperioden 2021-2023:

- Säkra stabil drift och förvaltning
- Cybersäkerhet och Security Operations Center (SOC)
- Effektiva arbetsformer
- Stöd och verktyg för dataanalys
- IT-arkitektur och strukturkapital
- Stöd i verksamhetsutveckling
- Digitalisering och innovation

Riksbanken har beslutat och genomfört en utkontraktering av all IT-drift och support till CGI AB. Avtalet löper efter förlängning till dec 2026 med möjlighet att förlänga ytterligare men som längst till och med dec 2028.

En utkontrakterad IT-drift kräver en väldokumenterad och flexibel IT-arkitektur som går att flytta mellan olika driftleverantörer. Arkitekturen ska därför inriktas mot att vara standardiserad och enkel, så långt det är möjligt, utan att göra avkall på säkerhets- och tillgänglighetskrav. Det skapar goda förutsättningar för stabil drift och underlättar

[1] IT-verksamheten avser alla IT-aktiviteter som utförs inom Riksbanken.

transformationsprojekt när leverantörer ska bytas ut i framtiden. Detta ska dock inte vara hindrande för Riksbankens innovationsarbete.

Styrande principer

Följande styrande principer ska gälla för IT-verksamheten:

- Avdelning för IT- och digitalisering (IT-organisationen[2]) ska driva Riksbankens digitala utveckling och samtidigt leverera en robust och säker förvaltning av hög kvalitet.
- IT-satsningar ska utgå från verksamhetens behov och i första hand ska färdiga tjänster, funktioner eller IT-stöd köpas in. Egenutveckling ska endast ske för Riksbanksspecifika behov där väsentlig nytta kan påvisas eller en passande lösning inte finns att köpa.
- IT-organisationen ska vara nytänkande och drivande i att skapa förutsättningar för Riksbanken att testa nya lösningar i en stimulerande och innovativ miljö.
- IT-organisationen ska ha en helhetsbild över bankens alla IT-kostnader. Förvaltningen av IT-stödet ska utgå från verksamhetens processer.
- IT-säkerhetsnivån ska vara hög och anpassad till behoven inom olika områden samt utgå från de hanteringsklasser som gäller för Riksbankens information.
- IT-arkitekturen ska baseras på välkända och standardiserade lösningar samt vara styrande vid förändringar i IT-miljön. Nya lösningar kan prövas inom områden där säkerhetskraven så medger och där det finns ett behov av snabbare utveckling, t.ex. IT-arbetsplats och analysområdet. Användning av molntjänster ska alltid beaktas vid ny- och vidareutveckling.
- IT-organisationen ska ha egen kompetens inom strategiska verksamhetsområden för både IT och Riksbanken. Utkontraktering ska ske av IT-verksamhet som inte är specifik för Riksbanken och där det finns extern part som kan utföra verksamheten enligt Riksbankens krav och övergripande mål.
- Beslutade styrmodeller och arbetsprocesser ska användas för att leverera IT-tjänster effektivt och med tillräcklig kvalitet.

IT-organisationen

För att Riksbanken ska få ett stabilt, säkert och tillgängligt IT-stöd ska IT-organisationen ha kompetens för att kunna leverera inom följande tjänsteområden:

- stöd i verksamhetsutveckling och förändringsarbete
- digitalisering, innovation och nya teknologier
- IT-arkitektur och strukturkapital
- projektledning, metodstöd och kvalitetssäkring
- förvaltning av Riksbankens IT-stöd
- leverantörsstyrning och leveransuppföljning
- IT-drift och support
- IT-säkerhet och SOC
- internationellt IT-samarbete.

2 Hur ser behovet av IT ut hos Riksbanken?

2.1 Riksbanken

Riksbanken är Sveriges centralbank, en myndighet under riksdagen. Riksbanken har två huvuduppgifter: att upprätthålla ett fast penningvärde och att främja ett säkert och effektivt betalningsväsende.

Vi står nu inför ett relativt stort skifte till följd av strukturomvandlingen som pågår i det finansiella systemet världen över, inte minst inom området betalningar.

Sammantaget verkar vi i ett föränderligt och osäkert landskap och behöver vara förberedda på flera alternativa framtider. Vi måste skydda Sveriges ekonomi mot ökade risker och ha förmåga att ställa om verksamheten utifrån förändringar i omvärlden. Samtidigt behöver vi se till att vår arbetsplats följer med i tiden och drar nytta av de möjligheter som t.ex. teknikutvecklingen ger. I korthet så kan Riksbankens strategiska målbild sammanfattas till:

En nytänkande centralbank med hög beredskap

- **Nytänkande – i vårt tjänsteutbud, genom digitalisering/innovation och i vår kommunikation:** I våra verksamheter och på betalningsområdet, måste vi tänka nytt och anpassa vårt tjänsteutbud och arbetssätt till hur vår omvärld förändras. Vi ska använda de möjligheter ny teknik och ny information ger.

- **Hög beredskap – operationellt, finansiellt och i vår analys:** En utmaning för att nå hög beredskap är att upprätthålla en hög säkerhet och beredskap (inkl. cybersäkerhet) för våra kritiska system. Vår analys behöver vila på en robust grund, baseras på forskning och ligga i framkant med hög beredskap att snabbt svara upp mot nya utmaningar.

2.2 Framgångsfaktorer

Riksbankens målbild för 2019-2023 sammanfattas i nedanstående bild. Fem strategiska områden har identifierats där vi under de närmaste åren behöver ta nya vägar eller större steg framåt för att utveckla verksamheten samt uppnå vår målbild.

2.3 Utvecklingsbehov

Med utgångspunkt från Riksbankens strategiska plan 2019-2023 har följande områden med utvecklingsbehov identifierats inom Riksbankens verksamhet:

1. En betalmarknad för framtiden
2. Kommunikation i nya former
3. Stärkt beredskap
4. Uppdaterad omvärldsanalys
5. En utvecklande arbetsplats

Det kan konstateras att behoven och utvecklingsmöjligheterna hos Riksbanken går i linje med andra verksamheter i vår omvärld. Den snabba utvecklingen gör att en modern IT-organisation behöver balansera behoven av att vara mer snabbfotad och innovativ med att samtidigt kunna leverera stabilt och säkert IT-stöd på samma sätt som tidigare. En annan drivkraft som påverkar utveckling är digitaliseringen som framhåller att IT är en strategisk resurs och en förutsättning för att verksamheten ska lyckas, då alla verksamheter är beroende av IT i sitt dagliga arbete. Detta ställer krav på att IT-verksamheten blir en mer integrerad del i verksamhetsutvecklingen.

Utvecklingen går fort och drivkrafterna är många, t.ex. pandemin som har skapat stora förändringar i sättet att arbeta. Även kombinationen av sociala medier, molntjänster, mängden tillgänglig data och mobilitet har bidragit till att ytterligare öka möjligheterna och förändringstakten med hjälp av IT samtidigt som utmaningarna med att upprätthålla en tillfredställande IT-säkerhet blir allt större.

2.4 IT-verksamhetens bidrag

För att uppnå de övergripande målen i den strategiska planen och bidra till verksamhetens utveckling ska IT-verksamheten (IT) bidra med följande inom respektive område:

1. En betalmarknad för framtiden

- **Utvecklad analys av betalmarknaden:** IT ska stötta och bidra i analysen av omvärlden samt tillhandahålla en IT-miljö som möjliggör modern kommunikation.

- **Framtidens betalinfrastruktur:** IT deltar aktivt och bidrar med djup IT-kompetens och säkra miljöer i utvecklingsprojekt och förvaltning av framtidens betalinfrastruktur.

- **Anpassningar i RIX:** IT deltar aktivt i arbetet med RIX uppgraderingar, i nära samverkan med verksamheten och aktuella leverantörer, samt med att vidareutveckla användningen av IT-stödet och säkerställa robusthet (säkerhet och tillgänglighet).

- **Riksbankens roll i kontantförsörjningen:** IT deltar aktivt i etableringen av nya utlämningsställen och i vidareutvecklingen av aktuella IT-stöd.

- **E-kronan:** Projektet om digitala centralbankspengar går in i en ny fas och IT deltar i projektet med att utveckla en konkret pilot för hur en e-krona skulle kunna vara

utformad och fungera – för att möjliggöra ett framtida beslut om ett eventuellt införande.

2. Kommunikation i nya former

• **Rätt kommunikation till rätt målgrupper:** IT bidrar i arbetet med att förenkla och hitta nya innovativa sätt att kommunicera med aktuella målgrupper.

• **Ökad närvaro i sociala medier och Nya mötesplatser:** IT bidrar i arbetet med att hitta nya innovativa och digitala former för att nå en bredare allmänhet.

3. Stärkt beredskap

• **Höjd nivå informationssäkerhet/cybersäkerhet**: IT stärker sin kompetens och resurser inom området, etablerar en modern SOC med nya verktyg och säkerställer snabb tillgång till expertstöd (i form av ett Security Incident Response Team (SIRT)) om behovet för det uppstår. Målbilden är att vidareutveckla SOC till ett Cyber Resilience Center (CRC), för att ytterligare utvidga och förstärka Riksbankens kompetens, fokus och arbete med IT- och cybersäkerhet[3].

• **Intern krisberedskap/kontinuitet:** IT ska tillsammans med vår driftleverantör tillhandahålla en hög nivå av säkerhet så att Riksbanken är bättre rustad för kris och med förbättrad kontinuitet.

• **Möta ökade krav på totalförsvar**: IT kommer under perioden ytterligare utöka beredskap och stärka skydd för våra IT-stöd utifrån ökade krav och hot från omvärlden.

• **Upprätthålla en hög finansiell krisberedskap:** IT-tjänsterna ska vara rustade för att klara kriser genom att säkra hög tillgänglighet till vår IT-infrastruktur och nödvändiga IT-tjänster.

4. Uppdaterad omvärldsanalys

• **Penningpolitiken mot normalisering i ny miljö:** IT underlättar arbetet med att fördjupa analysen med nya moderna IT-stöd som effektiviserar och underlättar arbetet med att komma åt och analysera information/data.

• **Finansiell stabilitet i ett nytt finansiellt landskap:** IT tillhandahåller en modern data- och analysplattform för stöd i analysarbetet.

• **Centralbanken och hållbarhet:** IT säkerställer krav på hållbarhet och minskad klimatpåverkan via kravställning i alla våra IT-upphandlingar.

• **Uppgraderad informationsförsörjning:** IT tillhandahåller moderna verktyg och anpassat stöd till olika användarkategorier via en modern data- och analysplattform.

[3] Detta bl.a. genom att förvalta och vidareutveckla Riksbankens IT-säkerhetsarkitektur, utveckling av Security Services samt stöd för Security Development Lifecycle (SDLC) och DevSecOps. DevSecOps är en uppsättning av metoder som kombinerar och binder samman mjukvaruutveckling (Dev), IT-säkerhet (Sec) och IT-drift (Ops) för att förkorta tid för systemutveckling och tillhandahålla kontinuerlig leverans med hög säkerhet och mjukvarukvalitet.

5. En utvecklande arbetsplats

• **Effektiva och hållbara arbetsformer:** En projektstödsfunktion införs för att effektivisera och stötta i projektarbete. IT bidrar med modernisering av våra mötesformer, vidareutvecklar former för effektivt och säkert distansarbete och hur vi arbetar med ständiga förbättringar i den löpande verksamheten bl.a. med utgångspunkt i de erfarenheter vi fått i samband med pandemin.

• **Moderna och effektiva IT-stöd:** Genom olika digitaliseringsinitiativ ska vi testa och ta till oss de möjligheter som ny teknik kan ge oss, hitta var vi kan skapa utrymme och minska risker genom att automatisera/robotisera processer, och skapa förutsättningar för mer innovation överlag.

• **Strategisk kompetensförsörjning:** IT ska aktivt bidra till att stärka alla medarbetares IT-kompetens samt öka medvetenheten och inspirera till att se nya möjligheter med hjälp av ny teknik. IT ska stärka sin kompetens och resurser inom de identifierade strategiska kompetensområdena. Vi behöver blanda olika kompetenser i tvärfunktionella team för att utnyttja all vår potential och lösa de nya utmaningarna. Kombinationen av djup sakkunskap, förmågor, inställning och engagemang är avgörande.

Utifrån ovanstående strategiska målbild har följande huvudområden identifierats som IT-verksamheten behöver fokusera på för att uppfylla verksamhetens behov under perioden 2021-2023:

- Säkra stabil drift och förvaltning
- Cybersäkerhet och SOC
- Effektiva arbetsformer
- Stöd och verktyg för dataanalys
- IT-arkitektur och strukturkapital
- Stöd i verksamhetsutveckling
- Digitalisering och innovation

Inom ramen för Riksbankens strategiska projekt och i den årliga verksamhetsplanen beskrivs aktiviteter för varje område som detaljplaneras och löpande följas upp för att IT-verksamheten ska nå den strategiska målbilden till 2023.

3 IT-styrning

3.1 Styrande principer för IT-verksamheten

För att säkra att varje beslut driver Riksbankens IT-verksamhet i linje med denna IT- och digitaliseringsstrategi ska följande styrande principer gälla. Principerna ska vara ett stöd i det dagliga arbetet och vara vägledande vid beslut och prioritering avseende IT inom Riksbanken.

- Avdelning för IT- och digitalisering (IT-organisationen) ska driva Riksbankens digitala utveckling och samtidigt leverera en robust och säker förvaltning av hög kvalitet.
- IT-organisationen ska vara nytänkande och drivande i att skapa förutsättningar för Riksbanken att testa nya lösningar i en stimulerande och innovativ miljö.
- IT-satsningar ska utgå från verksamhetens behov och i första hand ska färdiga tjänster, funktioner eller IT-stöd köpas in. Egenutveckling ska endast ske för Riksbanksspecifika behov där väsentlig nytta kan påvisas eller en passande lösning inte finns att köpa.
- IT-organisationen ska ha en helhetsbild över bankens alla IT-kostnader. Förvaltningen av IT-stödet ska utgå från verksamhetens processer.
- IT-säkerhetsnivån ska vara hög och anpassad till behoven inom olika områden samt utgå från de hanteringsklasser som gäller för Riksbankens information.
- IT-arkitekturen ska baseras på välkända och standardiserade lösningar samt vara styrande vid förändringar i IT-miljön. Nya lösningar kan prövas inom områden där säkerhetskraven så medger och där det finns ett behov av snabbare utveckling, t.ex. IT-arbetsplats och analysområdet. Användning av molntjänster ska alltid beaktas vid ny- och vidareutveckling.
- IT-organisationen ska ha egen kompetens inom strategiska verksamhetsområden för både IT och Riksbankens. Utkontraktering ska ske av IT-verksamhet som inte är specifik för Riksbanken och där det finns extern part som kan utföra verksamheten enligt Riksbankens krav och övergripande mål.
- Beslutade styrmodeller och arbetsprocesser ska användas för att leverera IT-tjänster effektivt och med tillräcklig kvalitet.

3.2 IT-styrning

I arbetet med att få IT-verksamheten att fungera så bra som möjligt krävs en övergripande styrning av IT-satsningar med tydliga regler och beslutsvägar. Det bidrar till att Riksbanken kan använda sina IT-tillgångar på bästa sätt och hantera risker på ett medvetet sätt. Då IT-satsningar normalt påverkar fler områden inom Riksbanken krävs en väl etablerad samverkan kring beslut och prioritering av IT-satsningar. IT- och Digitaliseringskommitténs (IDK) roll blir därför central för att säkra att IT-verksamheten går i linje med verksamhetens behov.

I nedanstående matris beskrivs varje beslutstyp som påverkar IT, uppdelat på vem eller var beslut fattas, vilka som ska bidra och påverka samt hur beslut kommuniceras.

Beslut	**Vem eller var fattas beslut?**	**Rådgöra med inför beslut**	**Kommunicera**
IT- och digitaliseringspolicy	Direktion	IDK, LG	Alla, nås via Banconätet
IT- och digitaliseringsstrategi	Direktion	IT-chef, IDK, LG	Alla, nås via Banconätet
IT-budget	Direktion	IT-chef, IDK, LG	AID samt berörda verksamhetsområden och förvaltingsobjekt
Nytt eller förändrat verksamhetsstöd	Avdchef/Direktion[4]	IT-chef, IDK, Architecture & Security Board (ASB) [5]	AID samt berörda verksamhetsområden, förvaltningsobjekt och projektstödsfunktionen
Prioriteringar mellan projekt eller aktivitet	AID Avdchef[6]	IT-chef, IDK, LG, projektstöds-funktionen	AID samt berörda verksamhetsområden och förvaltningsobjekt
Förändrad funktionalitet i befintligt IT-stöd	Objektägare (Avdchef/Direktion)	AID, ASB, berörda förvaltningsobjekt	AID, Projektstödsfunktionen samt berörda förvaltningsobjekt via protokoll etc.
IT-arkitektur	IT-chef	ASB, IDK, LG	AID, delar relevanta för alla nås via Banconätet, relevanta delar till objektägare
IT-säkerhet	Avdchef Säkerhetsskyddschef	ASB, objekts- eller, informations-ägare, IT-chef, Riskchef, CISO, IDK, LG, SÄK	AID, vissa delar alla via Banconätet, delar till objektägare

I samband med den årliga budgetprocessen samlas samtliga IT-behov in via verksamhetsplaner och förvaltningsplaner. Därefter prioriteras samtliga efterfrågade IT-satsningar för nästa år och beskrivs i en gemensam IT-plan för Riksbanken. Planen förvaltas av projektstödsfunktionen och följs sedan upp och verifieras inom IDK, samt omprioriteras

[4] Regel för Riksbankens projekt och uppdragsstyrning

[5] AVS/IT har etablerat Architecture & Security Board (ASB) i syfte att säkerställa att de förändringar som görs i IT-stödet följer denna strategi och riktlinjer för arkitektur och IT-säkerhet samt görs på ett kostnadseffektivt sätt. ASB består av olika IT-kompetenser och agerar bollplank och rådgivare till verksamheten och projekt i frågor kopplade till arkitektur och IT-säkerhet samt styr arbete med arkitektur och IT-säkerhet.

[6] Arbetsordning och instruktion för Sveriges riksbank

vid behov. Samtliga vidareutvecklings- och förvaltningsaktiviteter drivs inom ramen för de fastställda förvaltningsobjekten.

3.3 Finansiering av IT-verksamheten

I arbetet med att vidareutveckla och underhålla IT-verksamheten inom Riksbanken krävs löpande satsningar i ny IT-infrastruktur samt i nytt och förbättrat IT-stöd. Finansiering av IT-verksamheten inom Riksbanken avser även löpande förvaltningskostnader för att driva och underhålla IT-verksamheten.

I syfte att skapa överblick och en helhetsbild kring kostnader för IT-verksamheten och för att undvika suboptimering ska:

- IT-organisationen ha en helhetsbild av bankens alla IT-relaterade investeringar och förvaltningskostnader. Under året samlas underlag *löpande* in till budgetprocessen. Budgetarbetet genomförs enligt Riksbankens budgetprocess.
- all licens- och avtalshantering ska ske i nära samarbete mellan IT-organisationen och verksamheten. Detta för att säkerställa en kostnadseffektiv, enhetlig och hållbar IT-miljö.

Förvaltningsobjekten ska ha den samlade kompetensen kring ingående verksamhetsområde och dess aktuella IT-stöd, med deltagare både från verksamheten och från IT-organisationen. Målet är att respektive förvaltningsobjekt ska planera och följa upp aktuell funktion, kostnader, avtal och licenser.

IT-kostnader för varje verksamhetsprocess ska tydliggöras och ställas i relation till den nytta som IT-stödet genererar. Utifrån detta kan sedan möjligheten att ytterligare rationalisera och konsolidera Riksbankens IT-stöd utvärderas.

3.4 Uppföljning av IT-verksamheten

Uppföljning ska säkerställa att IT-organisationen gör rätt saker för att stödja verksamheten i arbetet med att nå Riksbankens övergripande mål. Mätetal för IT ska vara möjliga att härleda till motsvarande mätetal i verksamheten samt säkerställa att IT- och digitaliseringsstrategin uppfylls. Arbetet med att följa upp dessa mätetal sker kontinuerligt i samband med tertialuppföljning.

IT-verksamheten ska mätas utifrån följande perspektiv:

- Leveranser där IT-organisationen bidrar till innovation och proaktivitet, samt till utveckling inom analysområdet.
- Relevanta områden från medarbetarundersökning som t.ex. effektivitetshinder
- Kundnöjdhetsenkäten (IT-enkäten)
- Avtalade servicenivåer avseende IT-stöd och leverans av IT-tjänster från aktuella leverantörer, samt uppfyllnad av ställda säkerhetskrav.

4 Leverans

4.1 Tjänster och Processer

4.1.1 Tjänster

IT-organisationen ska säkerställa att Riksbanken kan fullfölja sina uppgifter genom ett stabilt, säkert och tillgängligt IT-stöd. För att uppfylla Riksbankens behov behöver IT-organisationen leverera följande tjänster:

- **Stöd vid verksamhetsutveckling och förändringsarbete**

  IT-organisationen arbetar proaktivt och föreslår nya lösningar och agerar rådgivare i frågor kring hur verksamheten kan utvecklas med hjälp av IT. IT ansvarar för utveckling och/eller införande av nytt och förändrat IT-stöd. I detta arbete ingår bl.a. följande:

  - Kravhantering, beställning, upphandling och inköp
  - Hantering och strukturering av information
  - IT-arkitektur, IT-säkerhet, lösningsdesign och integration
  - Systemdesign och systemutveckling (vid egen utveckling)
  - Omvärldsbevakning

- **Digitalisering och innovation**

  IT-organisationen skapar förutsättningar samt driver innovationskultur, innovationsarbete och digital transformation för bättre effektivitet och användarupplevelse inom både IT och Riksbanken som helhet. IT bistår med struktur, verktyg och metodstöd för agilt och innovativt arbetssätt.

- **Projektstödsfunktion - projektledning, metodstöd och kvalitetssäkring**

  IT-organisationen leder, samordnar och kvalitetssäkrar Riksbankens projekt och uppdrag samt bidrar med metodstöd så att projektarbete utförs på ett enhetligt och effektivt sätt med god kvalitet. En projektstödsfunktion ger stöd och utbildning kring bl.a. metod, process och arbetssätt samt följer upp, samordnar och har helhetssyn över Riksbankens projektportfölj.

- **Förvaltning av Riksbankens IT-stöd**

  IT-organisationen tillgodoser verksamhetens krav på funktionalitet, tillgänglighet och IT-säkerhet genom en kontinuerlig förvaltning samt ny- och vidareutveckling av Riksbankens IT-stöd. Förvaltningen genomförs på ett kostnadseffektivt och strukturerat sätt i nära samverkan med verksamheten och aktuella leverantörer. Förvaltningsstyrningsfunktionen ansvarar för och bistår med stöd och uppföljning av det löpande arbetet med förvaltningsstyrning.

- **Leverantörsstyrning och leveransuppföljning**

  IT-organisationen styr, beställer och följer upp leveranser från Riksbankens IT-leverantörer och säkerställer att IT-stödet levereras enligt avtal.

- **IT-drift och support**

  IT-organisationen ansvarar för leveranser av IT-drift, applikationsdrift, arbetsplatsdrift och servicedesk.

- **IT-säkerhet och SOC**

  IT-organisationen säkerställer att efterfrågat IT-säkerhetsskydd finns på plats för att skydda Riksbankens IT-miljö. IT leder och samordnar allt operativt arbete kopplat till IT- och cybersäkerhet inom Riksbanken. IT arbetar löpande, i samverkan med verksamheten, med att identifiera säkerhetsbehov och genomföra säkerhetsåtgärder för att skydda Riksbankens IT-miljö. I arbetet med IT-säkerhet omfattas även kontinuitets- och katastrofplanering samt genomförande av tester i samverkan med verksamhet och leverantörer.

  IT-organisationen ansvarar för att löpande följa upp efterlevnad av krav och regelverk inom IT-säkerhetsområdet. Arbete utgår och styrs utifrån Riksbankens Ledningssystem för informationssäkerhet (LIS).

  IT-organisationen driver SOC för att kontinuerligt övervaka och skydda Riksbanken från säkerhetshot samt öka Riksbankens cyber resilience.

- **Arkitektursstyrning (ASB) och hantering av strukturkapital (EA-center)**

  IT-organisationen säkerställer att de förändringar som sker i IT-stödet följer denna strategi och riktlinjer för arkitektur och IT-säkerhet samt görs på ett kostnadseffektivt sätt. Detta görs genom Architecture & Security Board (ASB). ASB består av olika IT-kompetenser och agerar bollplank och rådgivare till verksamheten och projekt i frågor kopplade till arkitektur och IT-säkerhet samt styr arbete med arkitektur och IT-säkerhet.

  IT-organisationen hjälper till att säkerställa att Riksbankens strukturkapital (bl.a. process-, funktions-, informations- och systembeskrivningar) finns och hålls aktuella. Detta görs via Enterprise Architecture Center (EA-center). EA-center består av olika IT-kompetenser och Riksbankens Chief Data Officer (CDO) som tillsammans säkerställer att Riksbankens strukturkapital skapas och hålls aktuell så att Riksbankens verksamhet och IT-stöd enklare och snabbare kan förändras och vidareutvecklas.

- **Internationellt IT-samarbete**

  IT-organisationen säkerställer att Riksbanken följer och är anpassad till ESCB:s regelverk via deltagande i relevanta arbetsgrupper samt löpande omvärldsbevakar och samarbetar med BIS (i relevanta arbetsgrupper) och med andra centralbanker.

4.1.2 Styrande processer

För att leverera IT-tjänster effektivt och med tillräcklig kvalitet sker arbetet med hjälp av nedanstående beslutade styrmodeller och processer. Processer och styrmodeller ses över löpande för att arbetet ska bli effektivt och bidra till efterfrågad kvalitet.

- Riksbankens förvaltningsstyrningsmodell ska användas i arbetet med förvaltning av Riksbankens IT-stöd. Regeln Förvaltningsstyrning av Riksbankens IT-stöd[7] beskriver denna modell.

- Projektstyrningsmodellen Pejl ska användas vid arbete med projekt eller uppdrag anpassat efter projektets/uppdragets omfattning. Regel för Riksbankens projekt- och uppdragsstyrning beskriver besluts-, genomförande- och uppföljningsprocessen för dessa arbetsformer. Projektstödsfunktionen bistår med stöd till verksamheten under hela processen, från idé till genomförande och avslut av projekt och uppdrag.

- Ramverket ITIL[8] ska till beslutade delar användas i arbetet med drift, förvaltning och vidareutveckling av Riksbankens IT-stöd.

- RITS-processen[9] ska tillämpas vid större förändringar i Riksbankens IT-miljö.

- Regel för beredning av väsentliga verksamhetsförändringar ska tillämpas för att på ett proaktivt och effektivt sätt hantera Riksbankens operativa risker.

4.2 Arkitektur

IT-arkitekturens främsta syfte är att möjliggöra en sammanhållen, kostnadseffektiv, flexibel och framtidssäker leverans av IT-tjänster inom Riksbanken, med bibehållen funktionalitet, tillgänglighet och säkerhet. IT-arkitekturen ska även utgöra första linjens försvar i händelse av intrång och hot.

En utkontrakterad IT-drift kräver en väldokumenterad och flexibel IT-arkitektur som går att flytta mellan olika driftleverantörer. Arkitekturen ska därför inriktas mot att vara standardiserad och enkel, så långt det är möjligt, utan att göra avkall på säkerhets- och tillgänglighetskrav. Det skapar goda förutsättningar för stabil drift och underlättar transformationsprojekt när leverantörer ska bytas ut i framtiden.

För att vara kostnadseffektiv ska arkitekturen **återanvändas** i största möjliga mån vid ny- och vidareutveckling. För att uppnå det behöver **flexibilitet** och **skalbarhet** byggas in i arkitekturen så att den kan återanvändas och byggas ut utan att problem uppstår.

Dokumenterad, välkänt och **standardiserat** är ledord som ska genomsyra Riksbankens IT-arkitektur. På så sätt undviks onödiga kostnader och kompetens- och nyckelpersonsberoende. Detta ska dock inte vara hindrande för Riksbankens innovationsarbete.

Security and privacy by default and by design ska vara utgångspunkt vid all ny- och vidareutveckling för att säkerställa säkerhet i Riksbankens IT-stöd, uppfylla gällande regelverk samt öka Riksbankens cyber resilience.

[7] Regel Förvaltningsstyrning av Riksbankens IT-stöd

[8] Information Technology Infrastructure Library

[9] Regel för styrning av IT-säkerhet.

IT-organisationen ska etablera **löpande uppföljning** av efterlevnad av krav och regelverk inom IT-säkerhetsområdet. Detta arbete ska drivas av IT-säkerhetsansvarig inom IT-organisationen. Arbete utgår och styrs utifrån Riksbankens Ledningssystem för informationssäkerhet (LIS).

IT-organisationen ska driva en SOC för att kontinuerligt övervaka och skydda Riksbanken från säkerhetshot (som t.ex. obehörig åtkomst till information och resurser, säkerhetssårbarheteter och cyberattacker) samt öka Riksbankens cyber resilience. Målbilden är att vidareutveckla SOC till ett Cyber Resilience Center (CRC), för att ytterligare utvidga och förstärka Riksbankens kompetens, fokus och arbete med IT- och cybersäkerhet.

Behörighets- och identitetshantering samt **åtkomstkontroll** ska ingå som ett strategiskt område inom arkitekturen. Syftet är att kunna leverera en säker, tillförlitlig och spårbar åtkomst till Riksbankens IT-resurser och information.

Arkitekturen behöver också stå beredd när behov av och krav på **molntjänster** ökar. Dessa tjänster är ofta kostnads- och driftseffektiva men säkerhetsaspekten måste beaktas så att inte onödiga risker tas och att gällande regelverk följs.

Användning av molntjänster ska alltid beaktas vid ny- och vidareutveckling. Om användning av molntjänster blir aktuell ska i första hand färdiga tjänster (s.k. SaaS-tjänster, *Software as a Service*) utvärderas, och i andra hand plattformstjänster (s.k. PaaS-tjänster, *Platform as a Service*). Se bilaga 1, Riksbanken och molntjänster, för mer information om Riksbankens syn på molntjänster och deras nyttjande.

IT-organisationen ska styra Riksbankens arbete med arkitektur och IT-säkerhet genom Architecture & Security Board (ASB).

4.2.1 Den digitala arbetsplatsen

Den digitala arbetsplatsen ska vara modern och flexibel med **användaren**, **användarupplevelsen**, **mobilitet** och **säkerhet** i fokus. Den ska möjliggöra framtida arbetsformer och visionen om en användarvänlig, mobil och papperslös arbetsplats. Inom detta område behöver leveranser ske snabbt när behov uppstår. Styrande principer inom detta område är:

- Användarupplevelsen ska vara så **intuitiv** och **användarvänlig** som möjlig utan att äventyra säkerheten.
- Det ska finnas ökade **valmöjligheter** för mjuk- och hårdvara för att möta nya behov i takt med den tekniska utvecklingen inom området.
- Information och verksamhetssystem ska kunna nås från flera **olika enhetstyper** som ska vara anpassade för sina respektive ändamål och för **distansarbete**.
- Den digitala arbetsplatsen ska **separeras från känsliga verksamhetssystem.** Detta för att skapa förutsättning för snabba leveranser av ny funktionalitet, ökad användbarhet och bättre användarupplevelse inom området. Separationen innebär att de känsligaste IT-komponenterna ska placeras bakom ett åtkomstlager som kontrollerar relevanta parametrar innan åtkomst till IT-komponenten tillåts.

4.2.2 IT-plattformar

Riksbankens IT-stöd ska baseras på konsoliderade och tillgängliga IT-plattformar som möjliggör effektiv utveckling, drift och förvaltning. Här avses bl.a. utvecklings-, test-, drifts-, integrations-, databas- och analysplattformar. Styrande principer inom detta område är:

- IT-plattformar ska konsolideras till ett **fåtal plattformar** varav en ska utgöra förstahandsval inom respektive område.
- Allt **utbyte av information** mellan Riksbankens olika verksamhetssystem och med Riksbankens motparter ska ske via Riksbankens **integrationsplattform**, om inte annat standardiserat gränssnitt finns som t.ex. SWIFT.
- **Rätt behörigheter** är centralt för en säker IT-miljö. Ett stödsystem för styrning och uppföljning av behörigheter och åtkomst till applikationsplattform ska finnas och användas.

4.2.3 IT-infrastruktur

IT-infrastrukturen ska ge tillgång till Riksbankens IT-stöd med rätt åtkomstnivå och till godkända användare. IT-infrastrukturen ska präglas av **hög tillgänglighet** och kostnadseffektivitet med flexibilitet och skalbarhet i fokus. Styrande principer inom detta område är:

- IT-infrastrukturen ska vara **enkel och homogen** för minskad komplexitet och för hög flexibilitet, skalbarhet och tillgänglighet. Infrastrukturen ska standardiseras till ett fåtal välkända teknologier.
- Säkerhetsinfrastrukturen får undantas från principen om enkel och homogen infrastruktur. Denna infrastruktur tillåts vara mer komplex då den utgör första linjens försvar av Riksbankens IT-miljö. Det kan innebära att flera olika produkter används för att hantera t.ex. antivirus och brandväggar.

4.2.4 Information

Utgångspunkten för informationshantering ska vara visionen - rätt data i rätt läge.

Information ska vara tillförlitlig och sökbar samt lättillgänglig för användning och analys, både lokalt och på distans, utifrån användarnas behov och behörighet och informationens hanteringsklass.

Verktyg ska vara anpassade för olika användarkategorier med olika behov. Analysplattformen ska skapa förutsättning för nyttjande av AI/ML och nya analysmöjligheter.

Styrande principer inom detta område är:

- All information ska vara **informationsklassad** och lagringsplatser ska vara märkta med hanteringsklass. Detta ger ökade möjligheter till att skydda känslig information och införa flexiblare lösningar för mindre känslig information t.ex. via molntjänster.

- **Behörighet** till information ska hanteras och styras av informationsägaren som också har ett ansvar att följa upp åtkomsten till informationen.
- En plattform ska finnas för att för att **samla in, lagra och utbyta information**, strukturerad och ostrukturerad, på ett effektivt sätt och i överensstämmelse med gällande regelverk för hantering av personuppgifter.
- Ett stödsystem för **datamanagement** inklusive metadata ska införas för att underlätta analysarbetet.
- **Moderna verktyg** ska erbjudas för analys och visualisering av data och dessa ska vara anpassade för respektive ändamål och för användarnas behov.
- Förutsättningar ska skapas för en **ökad grad av självservice** för analys av stora och små datamängder.
- En plattform ska etableras för att hantera Riksbankens **strukturkapital** (bl.a. process-, funktions-, informations- och systembeskrivningar) på ett strukturerat och effektivt sätt.

IT-organisationen ska genom Enterprise Architecture Center (EA-center), i samverkan med Riksbankens Chief Data Officer (CDO), driva, styra och stötta i frågor kopplade till Riksbankens strukturkapital samt förvalta Riksbankens Systemkarta (inklusive Configuration Management Database, CMDB). Viktiga beskrivningar av Riksbankens verksamhet och IT ska finnas och hållas aktuella för att möjliggöra enklare och snabbare förändring och vidareutveckling av Riksbankens IT-stöd.

4.3 Organisation och kompetens

Den snabba utvecklingstakten i vår omvärld ställer ständigt nya och förändrade krav på IT samtidigt som kraven på leverans av ett stabilt och säkert IT-stöd kvarstår. Detta kräver en IT-organisation med kompetens och arbetssätt som möter upp mot dessa krav.

IT-organisationen ska kännetecknas av att vara verksamhetsorienterad och proaktiv samt att vara en nytänkande partner till verksamheten. IT ska arbeta tvärfunktionellt och tillsammans med verksamheten. Där så är lämpligt (t.ex. inom områden cybersäkerhet, analys, innovation och projektledning) ska kompetensnätverk etableras för att utöka och bredda kompetensen inom Riksbanken som helhet.

Inom IT-organisationen finns det idag kompetens inom följande viktiga områden:

- Utveckling och förändring av Riksbankens verksamhet, m.h.a. verksamhets- och IT-kunniga resurser som kan beskriva och översätta verksamhetens krav och behov till rätt IT-stöd.
- Innovation och digitalisering samt införande av agila och innovativa arbetssätt för en effektivisering av arbetet både på distans och på kontoret.
- Ledning och kvalitetssäkring av projekt och uppdrag samt stöd och utbildning kring projektarbete för att effektivisera och förbättra projektarbete.
- Metodstöd och processansvar för att säkerställa enhetliga, effektiva, innovativa och strukturerade arbetsformer.

- Förvaltning av Riksbankens IT-stöd tillsammans med verksamheten och aktuella leverantörer för att säkerställa stabil och säker drift och tillgänglighet av Riksbankens IT-stöd.
- Leverantörsstyrning- och leveransuppföljning för en effektiv hantering och samarbete med Riksbankens IT-leverantörer.
- Styrning och uppföljning av IT-drift och support för en stabil, säker och kostnadseffektiv IT-drift.
- Styrning och uppföljning av IT-säkerhet för att skydda Riksbankens IT-miljö mot säkerhetshot och cyberattacker.
- Säkerhetsövervakning och skydd, genom SOC, för att kontinuerligt övervaka och skydda Riksbanken från säkerhetshot samt öka Riksbankens cyber resilience.
- Utveckling och styrning av Riksbankens IT-arkitektur för att säkerställa att de förändringar som sker i IT-stödet görs på ett kostnadseffektivt sätt och följer arkitektur- och IT-säkerhetsriktlinjer.
- Utveckling och styrning av Riksbankens strukturkapital, genom EA-center, för att säkerställa att Riksbankens strukturkapital alltid finns på plats och hålls aktuellt så att Riksbankens verksamhet och IT-stöd enklare och snabbare kan förändras och vidareutvecklas.

För att kunna stödja verksamheten i deras utveckling och leverera efterfrågade tjänster, öka Riksbankens cyber resilience, strategiskt leda Riksbankens IT-utveckling samt vara en kompetent beställare och styra IT-leverantörer behöver IT-organisationen, utöver ovanstående, ytterligare förstärka kompetensen inom områdena projektledning, leverantörsstyrning, IT-arkitektur, systemförvaltning och test samt IT-säkerhet.

För att uppnå stabilitet, kvalitet och kontinuitet är det viktigt att det är egen anställd personal i roller avseende leverantörsstyrning och leveransuppföljning, arkitekturstyrning, IT-säkerhet, projektledning, förvaltningsledning samt i roller med kompetens kring kritiska verksamhetssystem.

4.4 Sourcing

För att IT-organisationen ska kunna leverera och ge rätt stöd till verksamheten är Riksbanken beroende av ett antal leverantörer som utför IT-tjänster.

Riksbanken har beslutat och genomfört en utkontraktering av all IT-drift och support till CGI AB. Avtalet löper efter förlängning till dec 2026 med möjlighet att förlänga ytterligare men som längst till och med dec 2028.

Utöver IT-drift och support, köps även andra IT-tjänster in som t.ex. konsultresurser vid behov av förstärkning.

För att få en rationell och kostnadseffektiv hantering av de IT-leverantörer som anlitas inom Riksbanken är det är viktigt att IT-organisationen är den sammanhållande länken.

Följande principer är styrande vid beslut och prioritering avseende IT-sourcing inom Riksbanken:

- Utkontraktering ska ske av IT-verksamhet som inte är specifik för Riksbanken och där det finns extern part som kan utföra verksamheten enligt Riksbankens krav och övergripande mål.
- IT-verksamhet som är specifik för Riksbanken eller där Riksbanken har bättre förutsättningar att utföra uppgiften än en extern part, ska bedrivas inom Riksbanken.
- IT-drift och support ska även fortsättningsvis vara utkontrakterad.
- I första hand ska färdiga tjänster, funktioner eller IT-stöd köpas in. Egenutveckling ska endast ske för Riksbanksspecifika behov där väsentlig nytta kan påvisas eller passande lösning inte finns att köpa. Användning av molntjänster ska alltid beaktas vid ny- och vidareutveckling. Aktuella tjänster ska alltid riskbedömas ur ett informations- och säkerhetsperspektiv.

Följande principer är vägledande och stödjande vid beslut och prioritering avseende IT-sourcing inom Riksbanken:

- Leverantörsstyrning och leveransuppföljning, styrande arkitektroller, IT-säkerhet, projektledning, förvaltningsledning samt roller med kompetens kring kritiska verksamhetssystem, ska bemannas med egen personal. Detta ger Riksbanken stabilitet, kvalitet och kontinuitet i IT-verksamheten.
- IT-organisationen ska ansvara för att beställa, upphandla och avtala IT-tjänster, IT-konsulter och övriga IT-relaterade inköp. Detta ger Riksbanken förutsättningar att effektivisera och rationalisera för att på så vis även hålla kostnaderna nere.
- Avtal med aktuella leverantörer ska alltid spegla och driva mot det som ska uppnås inom ramen för Riksbankens IT- och digitaliseringsstrategi. Betalningsmodeller ska då t.ex. premiera innovation eller en konsoliderad, standardiserad IT-miljö.
- Konsultstöd ska kunna avropas löpande vid behov av tillfällig förstärkning i projekt, förvaltning eller aktiviteter som kräver specifik kompetens.

5 Bilaga 1 - Riksbanken och molntjänster

Sammanfattning

Detta dokument är en bilaga till denna strategi som mer detaljerat beskriver Riksbankens syn och ställningstagande kring molntjänster. Målgruppen för denna bilaga är de hos Riksbanken som överväger att, eller arbetar med, planering, design, implementering, administration och underhåll av IT-tjänster med hjälp av molntjänster.

Användning av molntjänster väcker ofta många frågor; Är de tillförlitliga? Vilka är leverantörerna? Var finns informationen? Hur tillgängliga är tjänsterna? Är IT-säkerheten tillräcklig? Är man inlåst?

Syftet med denna bilaga är att kunna ta medvetna beslut under vilka förhållanden Riksbankens information ska tillåtas konsumeras i kommersiella molntjänster samt vilken typ av tjänst som ska väljas utifrån de olika behov som föreligger.

En förflyttning till molntjänster ska ske för att kunna ta del av fördelar och/eller förmågor som inte kan eller behöver tillhandahållas i egen eller i driftleverantörs infrastruktur.

Riksbanken ska bevaka vad som sker på området i Riksbankens omvärld t ex hos andra myndigheter och centralbanker, och följa med där det kan ge ett mervärde för Riksbanken.

Molntjänster finns tillgängliga i olika tjänstekategorier, Software as a Service (t ex Teams, WebEx), Platform as a Service (t ex ett databashotell) och Infrastructure as a Service (t ex en server, brandvägg). Beroende på kategori fördelas utförandeansvar mellan Riksbanken och leverantör. Observera att ansvaret för att tjänsten levererar och möter verksamhetsbehoven samt följer regelverk och lagstiftning alltid ligger på Riksbanken. Detta ansvar kan aldrig avtalas bort. Bilden nedan visar en modell över en IT-driftsmiljö med ansvarsområden för de olika tjänstekategorierna.

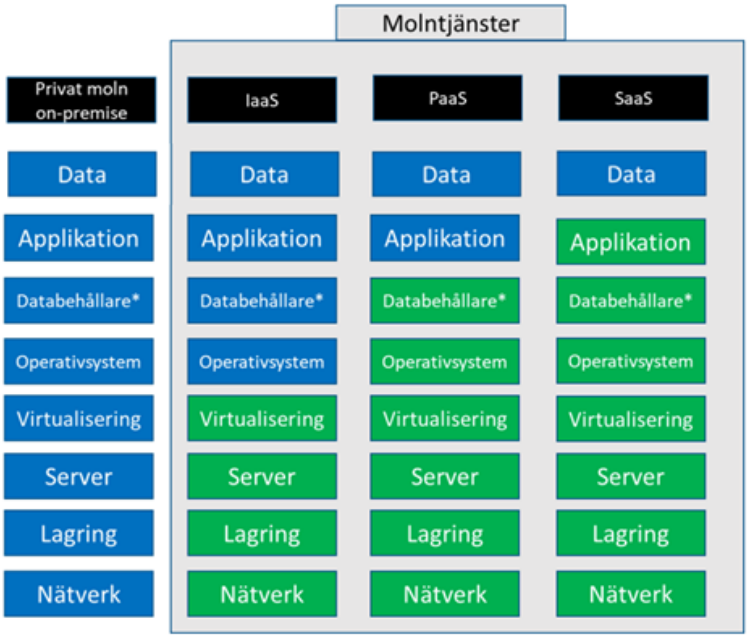

Bild 1 Blått är ansvar för Riksbanken och grönt driftansvar för molnleverantör. Riksbanken har alltid totalansvaret för att tjänsten levererar gentemot verksamhetsområdena.
*Avser s k Middleware och runtimemiljöer t ex Java resp. databasmotorer

För att bli en av Riksbanken godkänd molntjänstleverantör behöver leverantören passera Riksbankens RITS-process där de områden som molntjänstleverantören

ansvarar för (grönt) granskas utifrån ett IT-säkerhetsperspektiv innan eventuell beslut om förflyttning kan fattas.

Riksbankens inriktning är att som förstahandsval utvärdera möjlighet att placera Riksbankens information i de av Riksbanken godkända kommersiella molntjänsterna. Valet av tjänstekategori ska i första hand falla på SaaS (Software as a Service) och PaaS (Platform as a Service) och andra hand IaaS (Infrastructure as a Service).

Beslutet ska tas vid införande av nya tjänster/funktioner och IT-komponenter samt vid livscykelhantering av befintliga tjänster/funktioner och IT-komponenter. Detta gäller för information med informationsklass upp till och med ”Känslig”.

Information som av Riksbanken är klassificerad som ”Mycket känslig” är i dagsläget inte föremål för hantering i kommersiella molntjänster, undantag från detta kan beslutas av informationsägaren efter att en riskanalys gjorts och relevanta skyddsåtgärder vidtagits. Tillika är information/IT-system som lyder under säkerhetsskyddslagen inte heller föremål för en förflyttning till kommersiella molntjänster.

Tjänster som innehåller både Känslig och Mycket känslig information kan ändå vara föremål för att förflyttas till en molntjänst. Det kräver dock att det är möjligt att tjänsten kan ”delas” upp så att Mycket känslig information stannar i Riksbankens egna IT-miljöer (on-premise), s k hybridmoln.

Statlig utredning

I januari 2021 lämnade IT-driftsutredningen delbetänkandet Säker och kostnadseffektiv IT-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1). Enligt direktivet är syftet med utredningen att:

”…skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv IT-drift genom antingen samordnad statlig IT-drift eller genom tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av IT-drift”

Utredningen föreslår ändringar i Offentlighets- och Sekretesslagen (OSL) (2009:400), OSL, för utkontraktering av teknisk bearbetning och teknisk lagring av data. Riksbanken behöver bevaka utredningen och dess slutsatser för att avgöra om denna på något sätt kan underlätta beslut att göra förflyttningar till molntjänster.

Drivkrafter

De yttre förändringar som sker är en av Riksbankens stora drivkrafter för att nyttja molntjänster. Det förändrade säkerhetsläget leder till förändrade behov, där vissa är mycket svåra att möta utan att nyttja molnteknik. Samtidigt minskar utbud och support av mjukvaruprodukter för mer traditionella IT-driftsmiljöer.

De för Riksbanken viktigaste drivkrafterna för att nyttja molntjänster är:

- Kunna kommunicera och samarbeta, internt och externt, internationellt och nationellt, även vid krissituation.
- Öka flexibilitet och korta ledtider vid framtagande av verksamhetsstöd.
- Förbättrad skalbarhet och tillgänglighet.
- Förbättrad kontinuitet. Reducera störningar och förbättra IT-stabilitet samt möjliggöra alternativ vid störningar.
- Möjlighet att skapa nya tekniska funktioner och förmågor.

- Underlätta regelefterlevnad i form av att välja leverantörer vars plattformar har inbyggt stöd för regelefterlevnad, exempelvis GDPR.
- Alltfler on-prem produkter (dvs programvaror som är installerade lokalt i Riksbankens datahallar) upphör att erbjudas för installation i egna datahallar och Riksbanken vill kunna genomföra en kontrollerad förflyttning till molnet utan tvång och tidpress.
- Bevaka andra centralbankers och myndigheters förflyttning från lösningar on-prem till molnbaserade tjänster. Sker bl a genom ESCB samarbetet.

Definition

Molnarkitektur

Riksbankens molnarkitektur ska bygga på molndefinitionen enligt standarden ISO ISO/IEC 17788:2014.

Definitionen omfattar följande distributionsmodeller för molntjänster:

a) Publika moln (Public Cloud, privata aktörers molninfrastruktur med många kunder t ex Microsoft, Amazon, Google, IBM)
b) Gruppmoln (Community Cloud t ex statlig molninfrastruktur)
c) Hybridmoln (Hybrid Cloud, när minst två av de andra distributionsmodellerna kombineras)
d) Privata moln (Private Cloud, t ex CGI)

Publikt moln definieras av ISO som en distributionsmodell där molntjänster kan vara tillgängliga för vilken molnkund som helst och IT-resurserna kontrolleras av molntjänstleverantören.

För Riksbanken begränsas publika moln till de tjänster som tillhandahålls för företagskunder. Moln som riktar sig till konsumenter, t ex Hotmail, Gmail, Dropbox, iCloud, ingår därmed *inte* i begreppet publika moln för Riksbanken.

Distributionsmodell ska väljas efter väl utrett verksamhetsscenario där hänsyn tas till behov, IT-säkerhet och förvaltning. Olika arkitekturers påverkan på flexibilitet, skalbarhet, kontroll, tillgänglighet, kostnad, riskbedömning, laguppfyllnad10 och relevanta riktlinjer/regelverk11 ska ligga till grund för val av modell.

De olika distributionsmodellerna tillsammans med att det finns många aktörer som levererar tjänster för respektive distributionsmodell ger ökad komplexitet då det kan innebära att Riksbanken ökar antalet leverantörer att ha kontroll över istället för att ha en (1) leverantör som sköter allt. Det finns en överhängande risk för att applikationer och tillämpningar vid behov inte kan flyttas på ett enkelt sätt mellan de olika distributionsmodellerna och aktörerna. Det är därför viktigt att utvärdera och besluta om distributionsmodell och krav på molntjänster tidigt i processen för att säkerställa att

[10] T ex GDPR, Offentlighets- och Sekretesslagen, Säkerhetsskyddslagen

[11] T ex RITS, ESCB Cloud Policy

verksamhets- och säkerhetskrav uppfylls och att risker för inlåsningseffekter (både lock-in och lock-out) vid nyttjande av molntjänster undviks.

Huvudansvarig för en tjänst och dess innehåll såsom information/data, drift, underhåll, säkerhet, laguppfyllnad, revision mm kan aldrig avtalas bort. Det ansvaret faller alltid på Riksbanken.

Molndefinitionen bygger på tre grundläggande tjänstekategorier:

- SaaS, Software as a Service t ex Teams, WebEx
  Leverans av installerad mjukvara, applikationsfunktion. Applikation(er) tillgängliggörs till Riksbanken för olika typer av enheter och åtkomstsätt.
- PaaS, Platform as a Service t ex ett databashotell
  Tjänsteleverantör tillhandahåller standardiserad miljö för Riksbanken att driftsätta eller utveckla egna applikationer eller funktioner på.
- IaaS, Infrastructure as a Service t ex en server eller brandvägg
  Tjänsteleverantör tillhandahåller infrastrukturresurser, såsom server-, lagrings- eller nätverkskapacitet där Riksbanken själv ansvarar för att installation och hantering av operativsystem och mjukvara.

SaaS (Software as a Service) applikationer kan i många fall levereras av en tjänsteleverantör som i sin tur nyttjar underleverantörers tjänster för IaaS och PaaS. Dessa förhållanden ska framgå tydligt i samband med avtalstecknande för att granskning ska kunna ske utifrån IT-säkerhet och regeluppfyllnad. Detsamma gäller för nyttjande av PaaS-tjänster som kan vara beroende av IaaS-lösningar för att leverera funktionen.

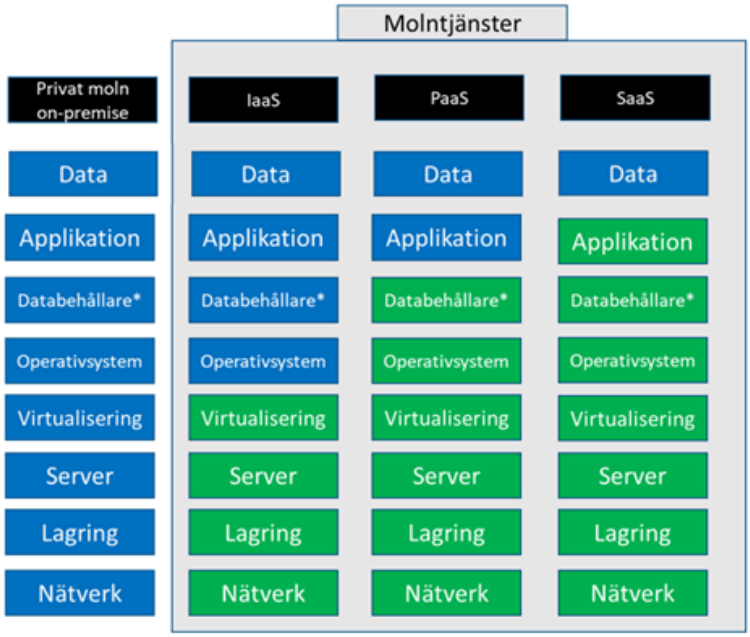

Bild 2 visar en modell över en IT-driftsmiljö med ansvarsområden för de olika tjänstekategorierna. Blått är ansvar för Riksbanken och grönt driftansvar för moln-leverantör. Riksbanken har alltid totalansvaret att tjänsten levererar gentemot verksamhetsområdena.
*Avser s k Middleware och Runtimemiljöer t ex Java resp databasmotorer

Utöver de tre grundläggande tjänstekategorierna har ISO kompletterat med ytterligare kategorier som i framtiden kan vara av intresse för Riksbanken såsom Compute as a Service (CompaaS), Data Storage as a Service (DSaaS), Network as a Service (NaaS), Communication as a Service (CaaS).

Utvärdering och uppföljning

Molntjänsteleverantörer

Drift i egen regi, eller outsourcad drift, ger goda förutsättningar att styra takten på utvecklingen t ex vid uppgraderingar. Beslutet ligger alltid hos Riksbanken.

Vid köp av tjänster minskar inflytandet över beslut och tidpunkt för en förändring då tjänsteleverantören tar över det ansvaret.

Tillämpning av molntjänster ska kontinuerligt utvärderas, inte minst med hänsyn till tjänsternas snabba utveckling.

Riksbankens utvärdering av molntjänsteleverantör ska bl a ta hänsyn till:

- Leverantörens uppskattade förmåga att kunna agera långsiktigt.
- Geografisk placering och möjlighet att styra var information hanteras och lagras samt identifiera ev tredjelandsproblematik ur ett GDPR-perspektiv.
- Förmåga att följa och införa för Riksbankens relevanta regler och riktlinjer12.
- Beredskap vid kris dvs förmåga att vid krisläge bibehålla leveransförmåga och tillgänglighet.
- Leveransförmåga med avseende på uthållighet, flexibilitet, snabbhet, möjlighet att skala upp och ut samt hålla fastställda SLA.
  Här ingår även leverantörens möjligheter att etablera fasta kommunikationslänkar mellan datacenter samt möjlighet till självservice för utökning av resurser t ex vid systemutveckling.
- Finansiell förmåga över tid dvs leverantörer ska vara ekonomiskt stabila företag med en stark marknadsposition.
- Leverantörens förmåga till efterlevnad av etiska och juridiska regelverk i sin affärsverksamhet.
- Hållbarhets- och miljöarbete.
- Attraktionskraft för partner och utvecklare att ta fram lösningar för Riksbanken.

Innan kontraktering ska bl a följande aktiviteter genomföras:

- Riskbedömning av leverantör med hjälp av bl a RITS
- Informations- och IT-säkerhetsbedömning inkl processer för att:
  - *Identifiera* - Kapacitet för att finna och hantera cybersäkerhetsrisker som kan uppstå mot system, människor, tillgångar, data och funktioner.
  - *Skydda* - Utveckla och implementera lämpliga skyddsåtgärder för att säkerställa leverans och tillgänglighet av kritiska tjänster.

[12] Såsom ledningssystem för informationssäkerhet och kriterier i RITS-processen, ISO27001 med tillhörande ISO27017 (Riktlinjer för säkerhetsåtgärder för molntjänster baserad på ISO/IEC 27002) och ISO27018 (Riktlinjer för skydd av personuppgifter i publika molntjänster som hanterar personuppgifter) och GDPR.

- *Upptäcka* - Utveckla och genomföra lämpliga aktiviteter för att identifiera förekomsten av en cybersäkerhetshändelse.
- *Respondera* - Utveckla och genomföra lämpliga aktiviteter för att vidta åtgärder vid upptäckt av en cybersäkerhetsincident.
- *Återskapa* - Utveckla och genomföra lämpliga aktiviteter för att upprätthålla planer för motståndskraft samt att återställa alla funktioner eller tjänster som har varit föremål för en cybersäkerhetincident.

- Upprätta ett ramverk för governance och servicenivåer där ansvar och skyldigheter för leverantör, eventuellt tredje part och Riksbanken tydliggörs.
- Riskbedömning av Riksbankens förmåga att styra och kontrollera leverantören.
- Definiera exitstrategi och avtalsmässiga förutsättningar för dess genomförande.
- Säkerställa att revision av molntjänster och leverantörer är möjlig och avtalad.

Arbetet med att godkänna en leverantör för att tillhandahålla tjänster till Riksbanken ska bedrivas i projektform med representanter både från IT och verksamheten. Detta för att få med alla intressenter i arbetet, få styrning, struktur och en tidplan för genomförande.

Strategisk målsättning är att godkänna minst två, helst tre, leverantörer för att undvika inlåsningseffekter och ha en fungerande exithantering. Existerande mindre molntjänster som Riksbanken konsumerar behöver också genomgå en genomlysning för att säkerställa att dessa når upp till Riksbankens krav på molnleverantörer.

Molntjänster hos vald leverantör

Styrande principer vid val av tjänstenivå

För att en förflyttning och nyetablering till en molntjänst ska vara möjlig måste informationsklassificering och kritikalitetsbedömning ha genomförts. Klassificeringen ligger alltid till grund för beslut. Beslut fattas av informationsägaren i samråd med ASB, RIE och SÄK.

Riskbedömningen som tidigare är gjord för leverantören kan återanvändas vid riskbedömning av leverantörens enskilda tjänster för att på så sätt underlätta förflyttningen. Endast nya risker som kommer med aktuell tjänst behöver då analyseras och hanteras.

Riksbankens inriktning är att vid införskaffande av nya tjänster och framtagande av nya tillämpningar (nyutveckling) som förstahandsval utvärdera möjlighet att placera Riksbankens information i de av Riksbanken godkända kommersiella molntjänsterna. Där så är möjligt bör man välja SaaS-tjänster istället för applikationsdrift i egna datorhallar.

Följande principer ska gälla för val av tjänstekategori vid anskaffning av IT-tjänster:

- Riksbanken ska alltid använda standardtjänster med SaaS som utgångspunkt
    - Finns en standardapplikation, som möter upp mot ställda krav och riskaptit ska den användas.
- Vid för Riksbanken unika tillämpningar ska:
    - PaaS tjänster nyttjas i första hand.
    - IaaS i andra hand då detta medför större eget åtagande för t ex drift.

Tjänster som innehåller både Känslig och Mycket känslig information kan vara föremål för att förflyttas till en molntjänst. Det kräver dock att det är möjligt att tjänsten kan ”delas” upp så att Mycket känslig information stannar i Riksbankens egna IT-miljöer (on-premise), s k hybridmoln. Fildelning och E-post är exempel på tjänster där det är teknisk möjligt att viss information eller personers brevlådor stannar i de egna datorhallarna. Att dela på ett IT-systems databas är däremot svårare. Då är den högsta klassen av information styrande var IT-tjänsten ska ligga.

Information och IT-system som lyder under säkerhetsskyddslagen är inte föremål för en förflyttning till kommersiella molntjänster i dagsläget.

För att kunna göra en förflyttning till en molntjänst är det viktigt att innan beslut tas utreda i vilken utsträckning Riksbanken har kontroll på krypteringsnycklar i tjänsten. Nyckelhanteringen är en viktig del av informationssäkerheten då det avgör vilka möjligheter en leverantör har att få åtkomst till data/information i tjänsten. Nyckelhanteringen ska hanteras inom ramen för RITS när IT-säkerhetskraven analyseras.

När en förflyttning är gjord ska IT-tjänsten fortsatt gå att återfinna i Riksbankens strukturkapital t ex i CMDB. Styrning och kontroll sker inom ramen för Riksbankens förvaltningsmodell.

Samtliga tjänstekategorier ska uppfylla följande kriterier:

- *Snabb skalbarhet.* Förmåga att skala upp och ner efter behov och i vissa fall per automatik.
- *Mätbarhet*. Resursanvändningen i tjänster och applikationer ska enkelt kunna mätas och följas upp avseende tillgänglighet och förbrukning. Kostnaderna ska kunna fördelas baserat på fast eller rörlig konsumtion och kunna härledas till t ex organisatorisk enhet, kostnadsställe.
- *IT-säkerhet, fysisk säkerhet, informationssäkerhet.*
    - Informationsseparation ska kunna påvisas mellan kunder som brukar samma tjänst.
    - Centrala cybersäkerhetsförmågor kring analys och upptäckt ska nyttjas.
    - Tjänster ska uppfylla Riksbankens krav på informations- och IT-säkerhet samt gällande regelverk och lagar t ex RITS, OSL, GDPR.
- *Laguppfyllnad*. T ex GDPR, OSL, Säkerhetsskyddslagen.

Statlig utredning

Just nu pågår en statlig utredning på området; IT-driftsutredningen (I 2019:03). *Riksbanken* behöver bevaka utredningen och dess slutsatser för att avgöra om denna på något sätt kan underlätta eller begränsa beslut att göra förflyttningar till molntjänster. Det gäller alla delar av organisationen som berörs av det utredningen omfattar t ex AID, RÄT, SÄK, RIE.

Utredningen syftar till att skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv IT-drift genom antingen samordnad statlig IT-drift eller genom tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av IT-drift.

Utredningen lämnade i januari 2021 sitt delbetänkande Säker och kostnadseffektiv IT-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1). I betänkandet ges en överblick av rådande situation med molntjänster där rättsläget idag är oklart. Den ger även en bild av vad omvärlden, främst Norden och Europa, gör på området samt en överblick av vad tidigare utredningar på området kommit fram till.

I betänkandet görs bedömningen att en myndighet som utkontrakterar IT-drift får anses ha lämnat ut de uppgifter som omfattas av utkontrakteringen till tjänsteleverantören. Om utkontraktering innebär att sekretessreglerade uppgifter röjs för tjänsteleverantören, så krävs det för att en utkontraktering ska vara förenlig med offentlighets- och sekretesslagen (2009:400), OSL, att utlämnandet sker efter en av myndigheten utförd skadeprövning, som utmynnat i slutsatsen att uppgiften kan lämnas ut, eller med stöd av en sekretessbrytande bestämmelse. Kritikalitetsbedömningen ligger alltid till grund för om informationen lämpar sig att lägga ut i en molntjänst eller ej. För Riksbankens del är dock information av klassen Mycket känsligt inte föremål att lägga i molntjänster enligt denna inriktning.

För att göra det lättare för offentlig verksamhet att fatta beslut kring en förflyttning till molntjänster inom och utom Sverige föreslår utredningen ändringar i OSL. Utredningen föreslår att det införs en ny paragraf 10 kap. 2 a § OSL. Den föreslagna paragrafen är en sekretessbrytande bestämmelse som tar sikte på utkontraktering av IT-drift.

10 kap. 2 a §
Sekretess hindrar inte att en uppgift lämnas ut till ett företag eller en annan enskild eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning. En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Utredningen föreslår vidare att 44 kap. 5 § OSL får en ändrad lydelse. Ändringen innebär att den i tryckfrihetsförordningen och yttrandefrihetsgrundlagen föreskrivna meddelarfriheten inskränks för den krets av personer som träffas av lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring av uppgifter.

44 kap. 5 §
Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer

6. av 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

Utredningen ska lämna sitt slutbetänkande den 15 oktober 2021. Den återstående delen av utredningen ska utreda samordnad drift för offentlig verksamhet.

Existerande IT-komponenter och förflyttning

Många organisationer gör idag en molnförflyttning av sina existerande IT-komponenter.

Förflyttningen kan ske på olika sätt och omfattar både applikationer och tjänster. Dessa kan t ex ersättas av en SaaS-tjänst eller byggas om från grunden för att kunna läggas ut i en molntjänst.

Vilken väg man väljer beror mycket på applikationens/tjänstens beskaffenhet och vilka behov och krav som finns. Inför beslut om förflyttning inom Riksbanken, ska det ha utretts vilka val som är lämpliga för att genomföra förflyttningen samt konsekvenserna för respektive val.

Exit

Förutsättningarna för avveckling av tjänst och tjänstenyttjande ska hanteras i avtal. Avtalet ska kunna avslutas i händelse av större avvikelse från principerna i utvärdering och uppföljning av tjänsteleverantören och tjänst.

Vid införande av nya tjänster och applikationer ska det ingå en plan för avveckling av tjänsten.

I samband med avveckling, oavsett grund (avtalsmässig eller livscykelmässigt), ska det finnas en plan för hur data och information ska hanteras vid exit. Planen ska beskriva hur data ska migreras till ny tjänst alternativt tas tillbaka till de egna datahallarna samt hur det säkerställs att all data och information inte kan återskapas hos leverantören i samband med avveckling av tjänsten.

Leverantören ska ha processer för att säkerställa att information inte finns kvar och kan återskapas.

Omvänt måste Riksbanken organisera sig för att leverantören förändrar eller drar tillbaka tjänster i snabbare takt än planerat. Tjänsterna i molntjänster kan förändras flera gånger under avtalstiden. Beredskap samt avtalsmässiga förutsättningar för att kunna hantera dessa förändringar behöver finnas på Riksbanken.

Det är av stor vikt att Riksbanken har en beredskap för att hantera leverantörers eventuella brister under avtalens giltighet, t ex finansiella brister, oegentligheter, etiska brister, så att tjänster i sådana situationer kan flyttas strukturerat till annan godkänd leverantör eller tillbaka till en lokalt installerad IT-tjänst i egna datorhallar (on-premise). En förflyttning kan bli aktuell t ex om leverantören visar sig ha ekonomiska svårigheter eller blir föremål för en brottsutredning och där Riksbanken gör bedömningen att det kan skada Riksbankens anseende.