Stockholm Stadshus AB
Implementering av Agresso - Genomgång av roller och ansvar för utvalda aspekter av intern kontroll i koppling till Tieto

The better the question. The better the answer.
The better the world works.

Building a better working world

Innehåll

Sammanfattning

Inledning
Stockholm stad har initierat ett projekt (SUNE) för att implementera ett gemensamt ekonomisystem för samtliga bolag inom Stockholm Stadshus AB. I upphandlingsfasen valdes ekonomisystemet Agresso och driften är utlagd på IT leverantören Tieto. Utveckling och underhåll av Agresso kommer att utföras av produktleverantören UNIT 4. Baserat på detta har Stockholm Stadshus AB uppdragit åt EY att utföra en kartläggning av vissa aspekter av internkontroll i koppling till Tieto och deras åtagande gentemot staden.

Scope
Uppdraget har omfattat en kartläggning av utformning och ansvarsfördelning av de generella IT kontrollerna logisk åtkomst och programförändring kopplat till Agresso. Områden inom IT-drift har även varit föremål för en mer schematisk kartläggning. Vårt uppdrag har genomförts i huvudsak genom intervjuer med nyckelpersoner inom Tieto, Stockholm Stad och Stockholm Stadshus AB. Arbetet har också inkluderat att samla in dokumentation över aktuella processer för att verifiera överlämningspunkter mellan de olika aktörerna. Då implementering av Agresso vid uppdragets genomförande fortfarande varit i projektfas, har inriktning och omfattning inte varit att genomföra någon mera detaljerad granskning via verifieringar och stickprov. Agresso-leveransen är fortfarande inom ramen för projektet och slutligt leveransgodkännande har ännu inte gjorts vilket innebär att exekvering och effektivitet av kontroller ej kunnat utvärderas.

Slutsats
Baserat på vår genomgång bedömer EY att det finns ändamålsenlig ansvarsfördelning mellan de olika aktörerna och att förutsättningar finns för etablering av god intern kontroll. Generellt har EY noterat att det finns en hög medvetenhet mellan parterna med väldefinierade överlämningspunkter.

För logisk åtkomst och programförändring har ansvarsfördelningen mellan samtliga parter kartlagts på ett övergripande plan i ett flödesschema och en HUKI matris (Huvudansvarig Utförande Informeras Kontrolleras) . EY bedömer att det finns en väldefinierad process framtagen med lämpliga processteg mellan aktörerna.

Rekommendation
Stockholm Stadshus AB bör fortsätta arbetet med att dokumentera samt fastställa processer och riktlinjer för att säkerhetsställa ändamålsenlig ansvarsfördelning. Stockholm Stadshus AB bör också i takt med implementering arbeta med att förankra processerna i olika delar, genom utbildning och information, för att säkerställa medvetenhet genom hela organisationen.

Sammanfattande kunskap från denna genomgång med tillhörande dokumentation ger vidare en bra grund för en, i ett nästa steg, mera detaljerad granskning då processer och kontroller finns slutligt fastställda och implementerade.

Inledning

Avgränsning

Kontrolltyper

1. Inledning
Avgränsning

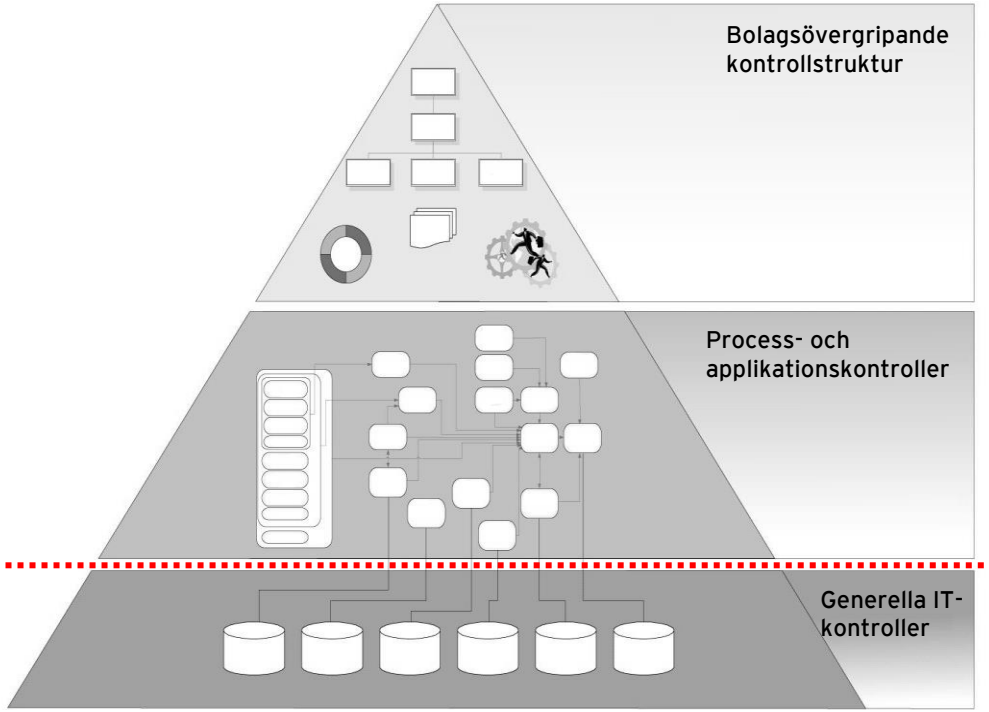
Uppdraget har omfattat en kartläggning av design och ansvarsfördelning av de generella IT kontrollerna logisk åtkomst, programförändring och IT-drift kopplat till Agresso. Kartläggningen har utförs i huvudsak genom intervjuer med nyckelpersoner på både Tieto och Stockholm Stads sida. I arbetet ingår också att samla in dokumentation över processerna för att verifiera överlämningspunkter mellan de olika aktörerna.

Då implementering av Agresso vid uppdragets genomförande fortfarande varit i projektfas, har inriktning och omfattning inte varit att genomföra någon mera detaljerad granskning via verifiering och stickprov. Agresso leveransen är fortfarande inom ramen för projektet och slutligt leveransgodkännande har ännu inte gjorts vilket innebär att exekvering och effektivitet av kontroller ej kunnat utvärderas.

1. Inledning

Kontrolltyper - Hur generella IT-kontroller är relevanta i revisionen

Inom ramen för denna granskning har EY valt att fokusera generella IT kontroller för att utvärdera kontroller inom logisk åtkomst, programförändringar och IT-drift. Vår granskning syftar framförallt till att kartlägga och bedöma risker som kan ha konsekvenser för den finansiella rapporteringen för Stockholm Stadshus AB. Granskningen har fokuserats på systemet Agresso



Bolagsövergripande kontroller som påverkar hela organisationen, t ex:

- Roller och ansvar
- Policys och riktlinjer
- Konsolideringsstrukturer
- Ledningens uppföljning
- Etc.

Specifika kontroller i finansiella rapporteringsprocessen, t ex:

- Avstämningar
- Kontroll av värderingar och bedömningsposter
- Attester/behörighet
- Analytiska kontroller
- Etc.

Generella IT-kontroller (ITGC) består av:

- Hantering av logisk åtkomst
- Hantering av system- och programförändringar
- IT-drift

Logisk åtkomst

2

Sammanfattning

Åtkomst till Agresso - övergripande

Ansvarsfördelning

Privilegierade access

Periodisk genomgång

2. Logisk åtkomst

Sammanfattning

EYs kartläggning har baserats på en genomgång av dokumentation/ policys som beskriver behörighetshanteringsprocessen från både Tieto samt bolagen inom Stockholm Stadshus AB, utöver detta har kartläggningen baserats på intervjuer med båda parter. Beskrivet nedan är de områden som har ingått i kartläggningen och på följande sidor beskrivs varje område mera ingående. Upplägg av nya användarkonton är beskrivet i appendix.

Logisk åtkomst

Fokus har varit att kartlägga olika nivåer för logisk åtkomst för Agresso, exempelvis parametrar för lösenord och användning av SSO-lösning.

Se sida 9 för ytterligare information.

Ansvarsfördelning

Fokus har varit att kartlägga och utvärdera huruvida ändamålsenlig ansvarsfördelning existerar inom behörighetsprocessen.

Då olika parter beställer, utvärderar och godkänner ny access i Agresso bedömer vi att ändamålsenlig ansvarsfördelning i processen existerar.

Se sida 10 för ytterligare information.

Privilegierad access

Fokus har varit att kartlägga hur privilegierade behörigheter hanteras, detta innefattar exempelvis systemadministratörskonton.

Se sida 11 för ytterligare information.

Periodisk genomgång

Fokus har varit att kartlägga hur periodiska genomgångar genomförs (både på applikationsnivå och infrastrukturnivå) . Vi har noterat att processer för dessa genomgångar ännu ej har implementerats.

Se sida 12 för ytterligare information.

Användarkonton

Fokus har varit att kartlägga hur godkännande och upprättande av behörigheteter hanteras för upplägg av nya behörigheter samt borttag av behörigheter. Denna process har kartlagts i ett processflöde samt en HUKI (Huvudansvarig, Utförande, Konsulteras och Informeras) -matris.

Se appendix sida 24-27 för ytterligare information.

2. Logisk åtkomst

Åtkomst till Agresso - övergripande

Åtkomst till Agresso - övergripande

Tieto ansvarar för att systemsäkerhetsinställningarna är implementerade i enighet med Stockholm stads krav. I Agresso kopplas varje användare till behörighetsroller och det är rollerna som styr vilken åtkomst användaren har i Agresso.

Det finns två olika typer av Agresso-åtkomster; Agresso Webb och Agresso Desktop. För att få åtkomst till Agresso måste användaren vara upplagt i stadens AD.

Agresso Webb
Agresso Webb nås via webbläsare och de flesta användarna har tillgång till Agresso web (ca 9000 användare). För Agresso web finns en SSO-lösning (Single Sign On).

Agresso Desktop
Agresso Desktop nås via stadens Citrix-miljö hos Tieto. Betydligt färre användare (ca 2000) har tillgång till Agresso desktop och för att få åtkomst till Agresso Desktop måste användaren vara kopplad till en specifik AD-grupp.

2. Logisk åtkomst

Ansvarsfördelning

Ansvarsfördelning

För att en användarbehörighet ska tilldelas finns det fyra aktörer inblandade; Tieto, Stadsledningskontoret, Volvo IT samt bolagen inom Stockholm Stadshus AB.

Varje bolag ansvarar för sina Agresso-användare och behörigheter. Bolagen utför beställning av ny/ ändrad behörighet genom att fylla i en behörighetsblankett. Per bolag finns det minst en behörighetsadministratör som granskar behörighetsblanketterna.

Behörighetsblanketten scannas och skickas sedan vidare till behörighetsregistrerarna på Tieto som granskar att informationen på blanketten är i enlighet med fördefinierade parametrar. Behörighetsregistrerarna på Tieto lägger sedan upp behörigheterna och skickar ett lösenord via epost till aktuell användare. För att ett upplägg av ny användare ska kunna göras i Agresso krävs det att det finns ett AD-konto, upplägg av AD-konton hanteras av Volvo IT.

Då olika parter beställer, utvärderar och godkänner ny access i Agresso bedömer vi att ändamålsenlig ansvarsfördelning i processen existerar.

2. Logisk åtkomst

Privilegierade accesser

Privilegierade accesser

Processen för att ansöka om privilegierad accesser ser i stort likadan ut som för vanliga konton och det är samma aktörer inblandade, men kräver i tillägg att objektsägare för Agresso även behöver skriva på behörighetsblanketten. När behörighetsblanketten skickas till Tieto krävs ett ytterligare godkännande innan accessen tilldelas.

I Agresso finns tre sorters privilegierad access; rollen SYSTEM, SYSAGR och SYSUTV. Rollen SYSTEM ger full behörighet i Agresso, denna roll ger rättigheter att uppdatera användarregister och behörighetsrollers menytillgång. Rollen SYSAGR ger inte rättigheter till att uppdatera användarregister och behörighetsrollers menytillgång men ger i övrigt samma behörighet som i rollen SYSTEM. SYSUTV används för utveckling och har exakta samma behörighet som SYSAGR.

Beslut om tilldelning av rollen SYSTEM och SYSAGR tas av objektsägaren för Agresso, vad gäller beslut om förlängning är det objektsägaren som tar detta beslut för rollen SYSTEM men för rollen SYSAGR kan detta beslut tas av behörig beställare hos Tieto.

Då objektsägaren av Agresso alltid måste vara inblandad vid ansökan av ny access bedömer vi att processen för hantering av privilegierade accesser är designad på ett lämpligt sätt. Även ansvarsfördelningen i tilldelning av privilegierade accesser bedöms vara ändamålsenlig.

2. Logisk åtkomst

Periodisk genomgång

Periodisk genomgång

Tieto har interna processer för hur höga behörigheter till exempelvis produktionsservrar hanteras. Enligt den definierade processen ska Stadsledningskontoret genomföra en periodisk genomgång av höga behörigheter en gång per kvartal, denna process har dock ej implementerats ännu.

Ansvar för genomgång av vanliga konton ligger på bolagena inom Stockholm Stadshus AB.

Programförändringar

3

Sammanfattning

Ansvarsfördelning

Periodisk genomgång

2. Programförändringar

Sammanfattning

EYs kartläggning har baserats på en genomgång av dokumentation/ policys som beskriver programförändringsprocessen från både Tieto samt bolagen inom Stockholm Stadshus AB. Utöver detta har karläggningen baserats på intervjuer med båda parter. Beskrivet nedan är de områden som har ingått i kartläggningen och på följande sidor beskrivs varje område mera ingående. Implementation av programförändringar är beskrivet i appendix.

Programförändringar

Fokus har varit att kartlägga hur testning, utveckling och godkännande hanteras för implementering av programförändringar. Denna process har kartlagts i ett processflöde samt dokumenterats i en HUKI-matris.

Se appendix sida 28-33 för ytterligare information.

Ansvarsfördelning

Fokus har varit att kartlägga att ändamålsenlig ansvarsfördelning existerar inom program-förändringsprocessen.

EY har kunnat verifiera att identifierad process möjliggör för ändamålsenlig ansvarsfördelning i programförändringsprocessen.

Se sida 15 för ytterligare information.

Periodisk genomgång

Fokus har varit att kartlägga hur programförändringar utvärderas efter implementering och inom vilken tidshorisont.

Se sida 16 för ytterligare information.

2. Programförändringar

Ansvarsfördelning

Ansvarsfördelning

Finansavdelningen inom Stadsledningskontoret ansvarar för förvaltningen av Agresso utifrån ett verksamhetsperspektiv. Tieto ansvarar för driften av systemet och UNIT 4 utvecklar systemet. För tillfället pågår SUNE projektet vilket innebär att projektet just nu styr och ansvarar för utrullningen men även förvaltning av systemet.

Det är bolagen som lägger beställningen och Stadsledningskontoret som verifierar beställningen mot behov och godkänner utifrån ett ekonomisk perspektiv. Beställningen skickas sedan vidare till Tieto som i sin tur tar över ägandeskapet av ändringen, verifierar beställningen mot SLA och godkänner för utveckling. Tieto står fortfarande kvar som ägare men beställningen skickas vidare till UNIT 4 för utveckling. Acceptanstest utförs av Stadsledningskontoret innan UNIT 4 implementerar förändringen och lämnar över ärendet till Tieto.

I och med att det finns fyra aktörer inblandade i beställning, testning och godkännande så kan EY verifiera att identifierad process möjliggör för ändamålsenlig ansvarsfördelning i programförändringsprocessen.

2. Programförändringar

Periodisk genomgång

Periodisk genomgång

Genomgång av programförändringar initieras först när de varit produktionssatt en viss fördefinierad tid. Det finns ingen definierad tidshorisont, men beroende på karaktär kan såväl kortare som längre tid väljas. Programförändringar utvärderas i PIR (Post Implementation Review) av Change Manager på Tieto, denna utvärderar programförändringen mot krav gällande budgeterat resursnyttjande och förväntade resultat kontra realiserat resultat.

IT-drift

4

Sammanfattning

Problem och incidenthantering

Schemalagda jobb

Backuphantering

Återläsningstest

4. IT drift

Sammanfattning

EYs kartläggning har baserats på en genomgång av dokumentation/ policys som beskriver IT drifts processen från både Tieto samt bolagen inom Stockholm Stadshus AB, utöver detta har kartläggningen baserats på intervjuer med båda parter. Beskrivet nedan är de områden som har ingått i kartläggningen och på följande sidor beskrivs varje område kort mer ingående. Genomgången har inte haft som inriktning att dra slutsatser kring ändamålsenlighet i relaterade processer

Problem och incidenthantering

Fokus har varit att kartlägga hur problem och incident hanteras och kommuniceras.

Se sida 19 för ytterligare information.

Schemalagda jobb

Fokus har varit att kartlägga hur ansvarsfördelning för schemalagda jobb ser ut samt processen för filöverföringen i integrationsmotorn.

Se sida 19 för ytterligare information.

Backuphantering

Fokus har varit att kartlägga hur backuper hanteras och hur ofta de utförs.

Se sida 20 för ytterligare information.

Återläsningstest av backup

Fokus har varit att kartlägga hur processen runt återläsningstest av backup utförs och hur ofta.

Se sida 20 för ytterligare information.

4. IT drift

Problem och incidenthantering & Schemalagda jobb

Problem och incidenthantering

Problem- och incidenthantering hanteras enbart av Tieto och är reglerat via SLA:er mot Stockholm Stad. Kommunikationen mellan Stockholm Stad och Tieto sker antingen via en portal, mail, telefon alternativt chatt direkt med supporten på Tieto.
Produktfel hanteras av produktleverantören UNIT 4. Varje månad skickas en sammanställning på samtliga problem som har hanterats av Tieto till systemägaren på Stockholm Stad. Incidentrapporter skickas till systemägaren och avdelningen för digital utveckling 10 dagar efter att incidenten har hanterats av Tieto.

Schemalagda jobb

Tieto ansvarar för att filer skapas enligt schema och säkerställer att innehåll i filerna inte förändras innan integration. Tieto säkerställer även övervakningen av integrationen via TEIS plattformen och att den fungerar. Allt finns reglerat i detalj via SLA:er mot staden och går något fel skickas mail till berörd aktör.

Tieto ansvarar inte för innehållet i filerna utan det ligger på leverantören. Överlämningspunkten är en FTP server (ftp.stockholm.se) och leverantören ansvarar för att filer laddas upp och fungerar.

4. IT drift

Backuphantering & Återläsningstest av backup

Backuphantering

Återläsning av backup är reglerat via SIKT-avtalet men går även skräddarsy efter behov. Det är Tieto som står för backuphanteringen och loggar förs över genomförda backuper med datum och resultat.

Om inget annat är överenskommet tas backuper varje dygn och full backup varje vecka. Var fjärde vecka förvaras backupen på en annan plats och skall överensstämma med avtalat säkerhetskrav. Backuper sparas i en generation.

Återläsningstest av backup

Återläsning av backup är reglerat via SLA:er mot Stockholm Stad. Avtalet säger att Staden har att rätt beställa återläsningstester men det finns inget krav på Tieto att leverera återläsningstest till Staden om detta ej är beställt.

I dagsläget har inte Staden lagt beställning på periodisk återläsning av backup och det är endast databasen som är vital, enligt information vi erhållit i samband med vår intervju.

Appendix

5

Logisk åtkomst

Programförändringar

5. Logisk åtkomst

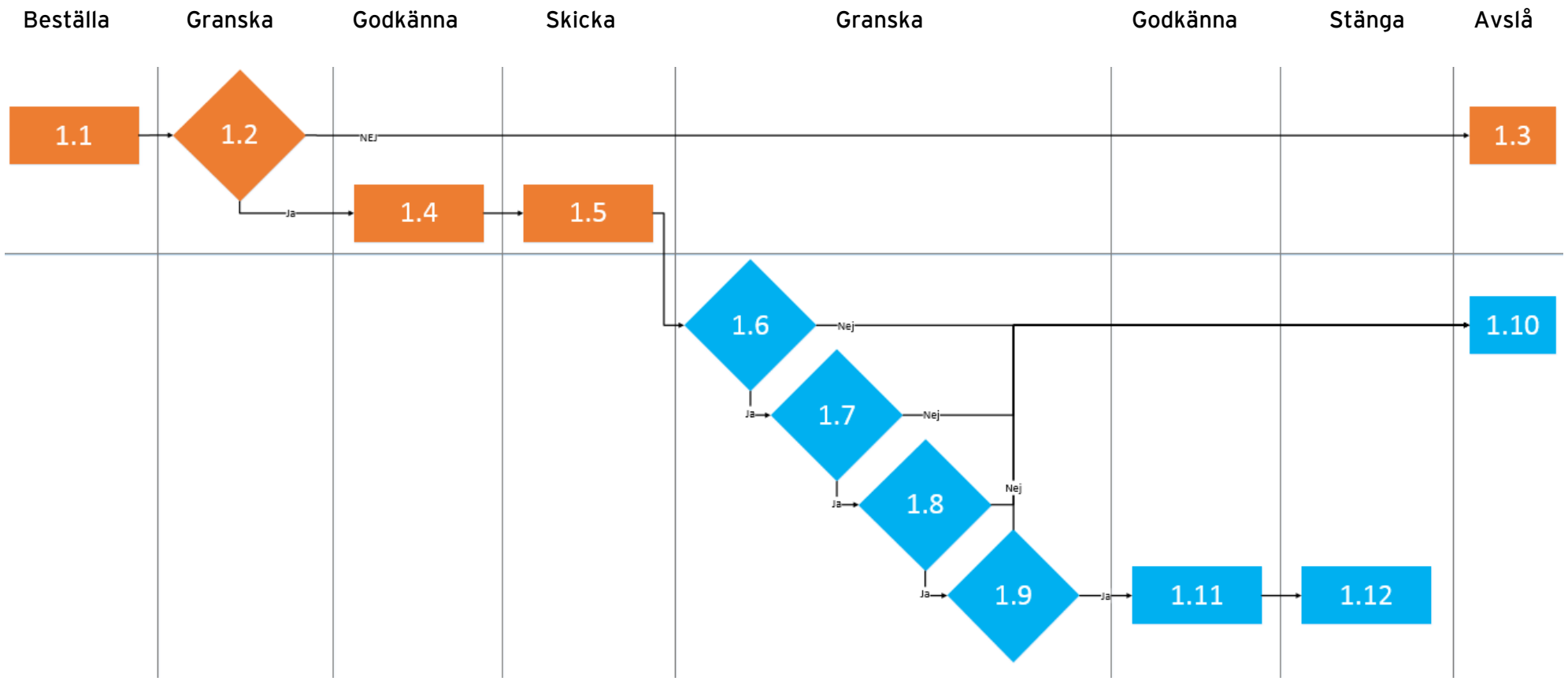
HUKI matris - upplägg av användarkonton

Baserat på intervjuer med Stockholm Stad och Tieto har EY tagit fram en HUKI (Huvudansvarig, Utförande, Konsulteras och Informeras) matris och flödesschema för att kartlägga ansvarsfördelningen för logisk åtkomst mellan de olika parterna.

	Aktiviteter	*Bolag inom Stockholm Stadshus AB (Beställare)*	*Bolag inom Stockholm Stadshus AB (Behörighets-administratör)*	*Tieto (behörighets-registrerare)*
1.1	Begära ny behörighet i behörighetsblanket	H / U	K / I	
1.2	Matcha roll mot beställd behörighet	I	H / U	
1.3	Beställning avslagen	I	H / U	
1.4	Godkänna och skriva under	I	H / U	
1.5	Scanna behörighetsblanket och maila beställning	I	H / U	
1.6	Verifiera om beställning är skickad från angiven mail	I	I	H / U
1.7	Verifiera om namnteckning matchar fullmakt	I	I	H / U
1.8	Verifiera om AD finns registrerat hos Volvo IT	I	I	H / U
1.9	Matcha beställning mot SLA	I	I	H / U
1.10	Beställning avslagen	I		H / U
1.11	Beställning registreras i Agresso			H / U
1.12	Användaruppgifter och lösenord skickas till beställare	I		H / U

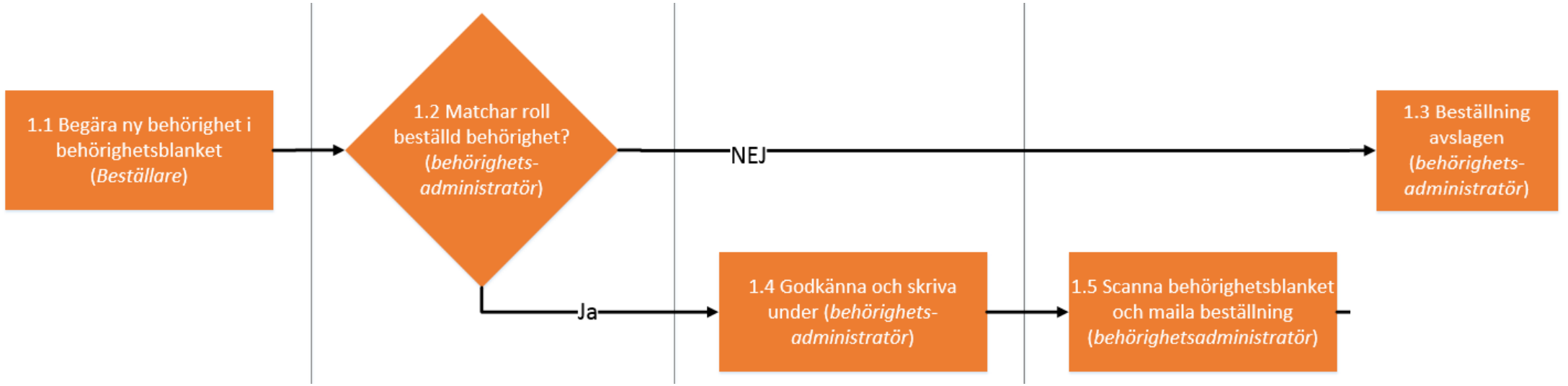
5. Logisk åtkomst

Flödesschema – upplägg av användarkonton (1/3)



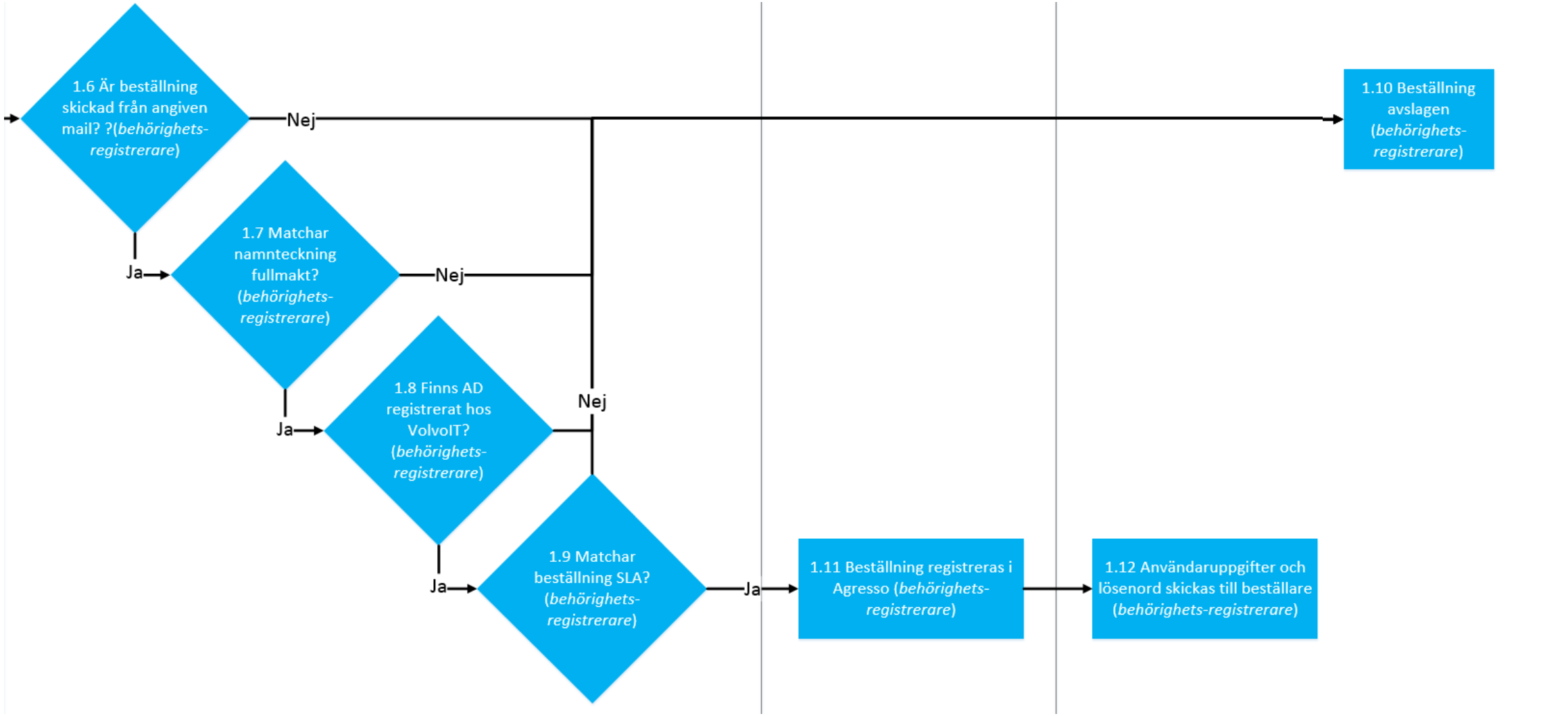
5. Logisk åtkomst

Flödesschema – upplägg av användarkonton (2/3)



5. Logisk åtkomst

Flödesschema – upplägg av användarkonton (3/3)



5. Programförändringar

HUKI matris – implementering av programförändringar (1/2)

Baserat på intervjuer med Stockholm Stad och Tieto har EY tagit fram en HUKI (Huvudansvarig, Utförande, Konsulteras och Informeras) matris och flödesschema för att kartlägga ansvarsfördelningen för programförändringarna mellan de olika parterna.

	Aktiviteter	*Bolag inom Stockholm Stadshus AB (Beställare)*	*Stadslednings-kontoret*	*Tieto (change designer)*	*Tieto (change manager)*	*Tieto (CAB)*	*UNIT 4 (change builder)*
1.1	Beställning av programförändring registreras i Excel	H / U	I				
1.2	Matcha beställda programförändring mot behovet	I	H / U				
1.3	Beställning avslagen	I	H / U				
1.4	Godkänna programförändring	I	H / U				
1.5	Maila beställning programförändring		H / U	I			
1.6	Verifiera om är beställning skickad från angiven mail			H / U	I		
1.7	Matcha beställning mot SLA			H / U	I		
1.8	Beställning avslagen	I	I	H / U	I		
1.9	Planera och registrera programförändringar i TONE (ärendehanteringsystem)			H / U	I		
1.10	Verifiera om CAB godkännande krävs för implementation			I	H / U	I	
1.11	Godkänna programförändring	I	I	I	H / U		

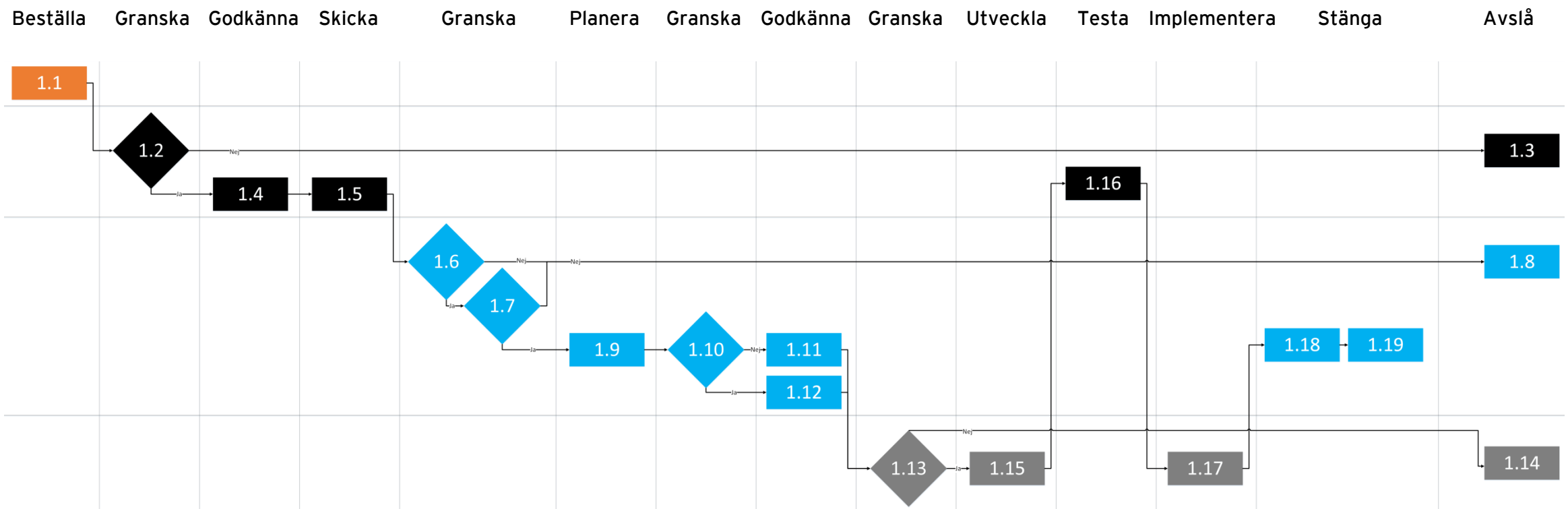
5. Programförändringar

HUKI matris – implementering av programförändringar (2/2)

	Aktiviteter	Bolag inom Stockholm Stadshus AB (Beställare)	Stadslednings-kontoret	Tieto (change designer)	Tieto (change manager)	Tieto (CAB)	UNIT 4 (change builder)
1.12	Godkänna programförändring i CAB möte	I	I	I	I	H / U	
1.13	Verifiera om beställd programförändring är tekniskt möjlig			I	I		H / U
1.14	Beställning avslagen	I	I	I	I		H / U
1.15	Utveckla programförändring			I	I		H / U
1.16	Acceptanstestning	I	H / U	I	I		I
1.17	Implementera programförändring	I	I	I	I		H / U
1.18	Granska ärende				H / U		
1.19	Utvärdera ärende PIR möte				H / U		

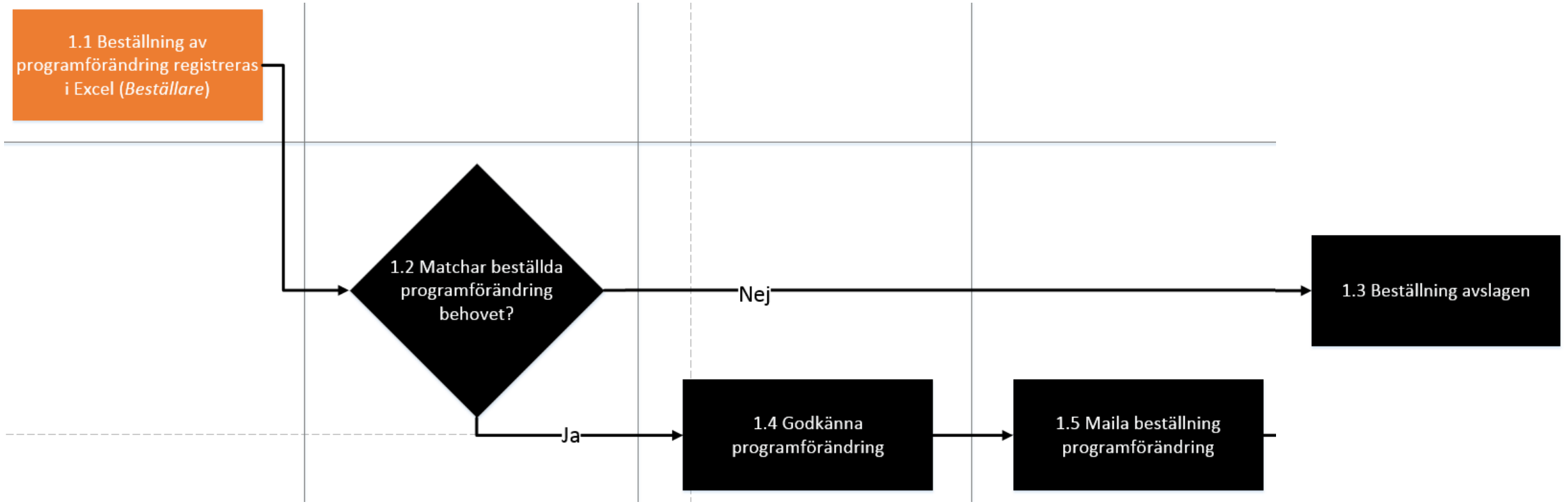
5. Programförändringar

Flödesschema – implementering av programförändringar (1/4)



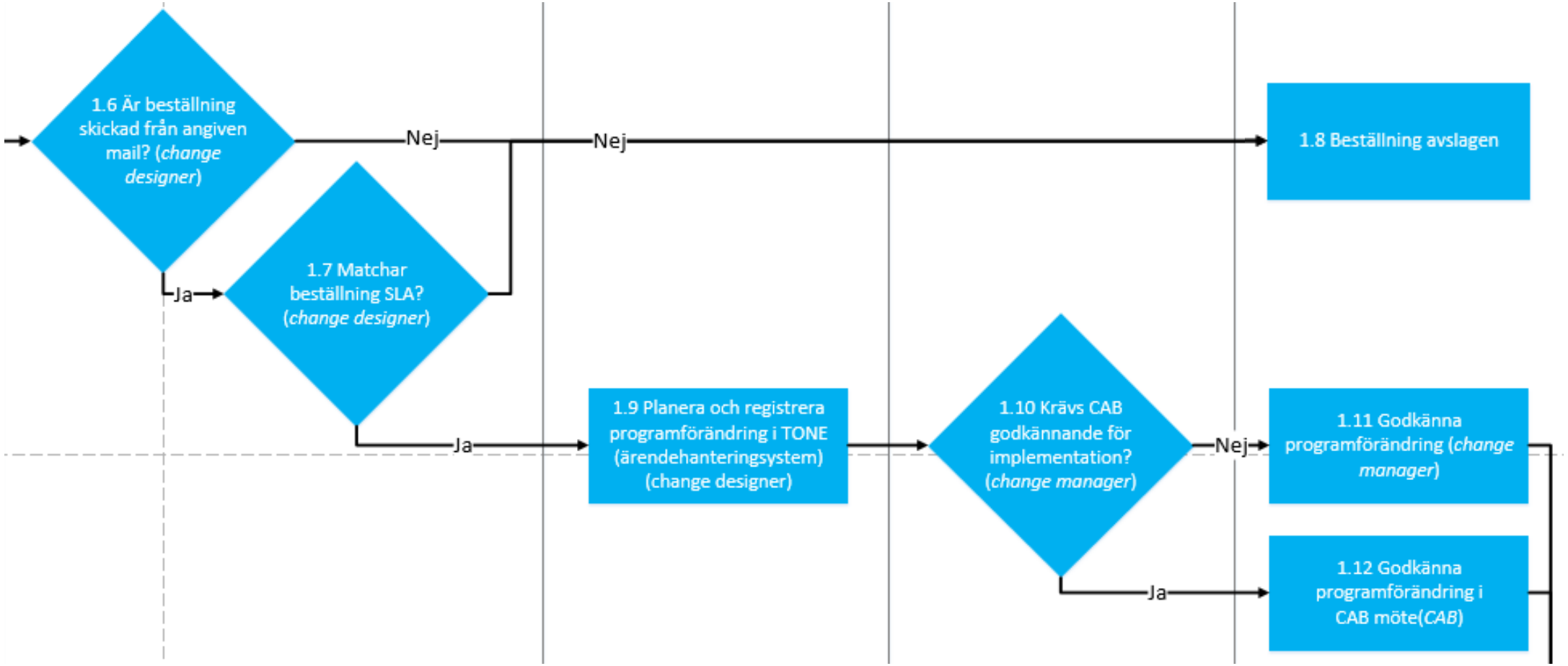
5. Programförändringar

Flödesschema – implementering av programförändringar (2/4)



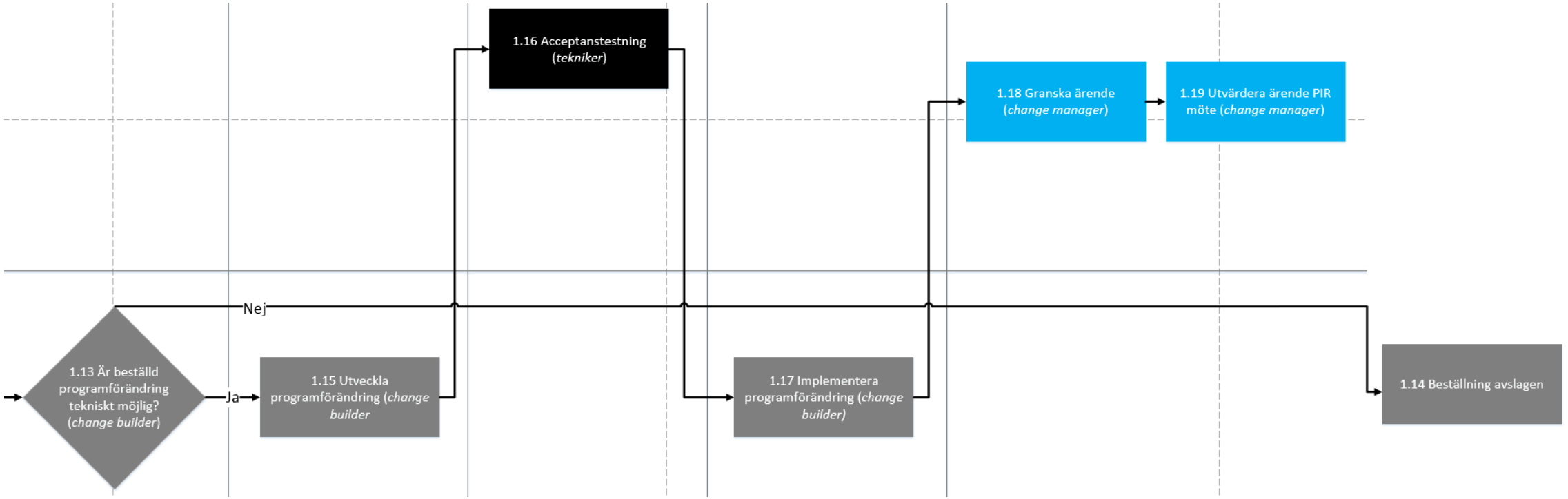
5. Programförändringar

Flödesschema – implementering av programförändringar (3/4)



5. Programförändringar

Flödesschema – implementering av programförändringar (4/4)




Tack!
The better the question. The better the answer.
The better the world works.
EY
Building a better working world