inera

Tillitsramverk

Identifieringstjänst SITHS

inera

Innehåll

Revisionshistorik

Version	Datum	Författare	Kommentar
1.0	2019-02-21	SITHS Policy Authority	Fastställt
1.1	2019-04-11	SITHS Policy Authority	Förtydligande om rollen Säkerhetsansvarig
1.2	2019-05-15	SITHS Policy Authority	Angett maximal giltighetstiden för certifikat i stycke 7.3.1

1. Inledning

1.1 Bakgrund och syfte

Identifieringstjänst SITHS ska tillhandahålla elektroniska identitetshandlingar för identifiering och signering för verksamhet och tjänster inom offentlig förvaltning för användning i tjänsten. I elektroniska identitetshandlingar ingår även de bärare[1] som behövs och tillitsramverket gäller även för dessa i tillämpliga delar.

Tillitsramverket syftar till att etablera gemensamma krav inom SITHS. Tillämpningen av tillitsramverket beskrivs i de rutiner som fastställs av SITHS PA.

För elektroniska identitetshandlingar för personer är kraven fördelade på olika tillitsnivåer. Detta svarar mot olika grader av teknisk och operationell säkerhet hos ansluten organisation som ger olika säkerhet i kontrollen av att en person, som tilldelas en elektronisk identitetshandling, verkligen är den han eller hon utger sig för att vara. Nivåindelningen motsvarar den som används i den internationella standarden ISO/IEC 29115. Kraven i detta tillitsramverk gäller tillitsnivå 2 till 4, där nivå 4 motsvarar den högsta nivån på processen för fastställande av identitet och skydd av elektroniska identitetshandlingar.

Kraven ska tolkas så att

a) om tillitsnivå inte är angiven ska kravet alltid uppfyllas, och
b) om tillitsnivå finns angiven, ska kravet uppfyllas på angiven nivå och högre.

1.2 Översikt

Detta dokument beskriver ramverket för SITHS som alla anslutna organisationer ska uppfylla. Tillitsramverket definierar grundkraven för SITHS Certifikatspolicy (SITHS CP) och tillsammans utgör de basen för alla övriga dokument som ingår i dokumenthierarkin.

1.3 Målgrupp

Målgrupp för dokumentet är SITHS Policy Authority (SITHS PA) samt Ansvarig utgivare och verksamhetsansvariga inom ingående organisationer.

[1] Exempel på bärare är kort och mobiltelefon

1.4 Identifiering

Detta tillitsramverk gäller för de elektroniska identitetshandlingar som utfärdas enligt nedanstående policy.

Namn för SITHS CP är:	{SITHS Certificate Policy}
Objektidentifierare (OID):	{ 1.2.752.74.8.1.1.1 }
Namn på detta tillitsramverk är:	{Tillitsramverk Identifieringstjänst SITHS }
Objektidentifierare (OID):	{ 1.2.752.74.8.2 }

1.5 Begrepp

Se dokumentet ”Termer och begrepp”.

2. Organisation och styrning

2.1 Övergripande krav

Organisation som vill ansluta sig till Identifieringstjänst SITHS, oavsett om det är direkt eller som tredjepart, ska vara en aktiv juridisk person. Direktansluten organisation ska i sin tillitsdeklaration ange vilka organisationer som den har tredjepartsanslutit.

Varje direktansluten organisation ska ha en skriftlig överenskommelse med varje organisation som den har tredjepartsanslutit

2.1.1 Regelverk

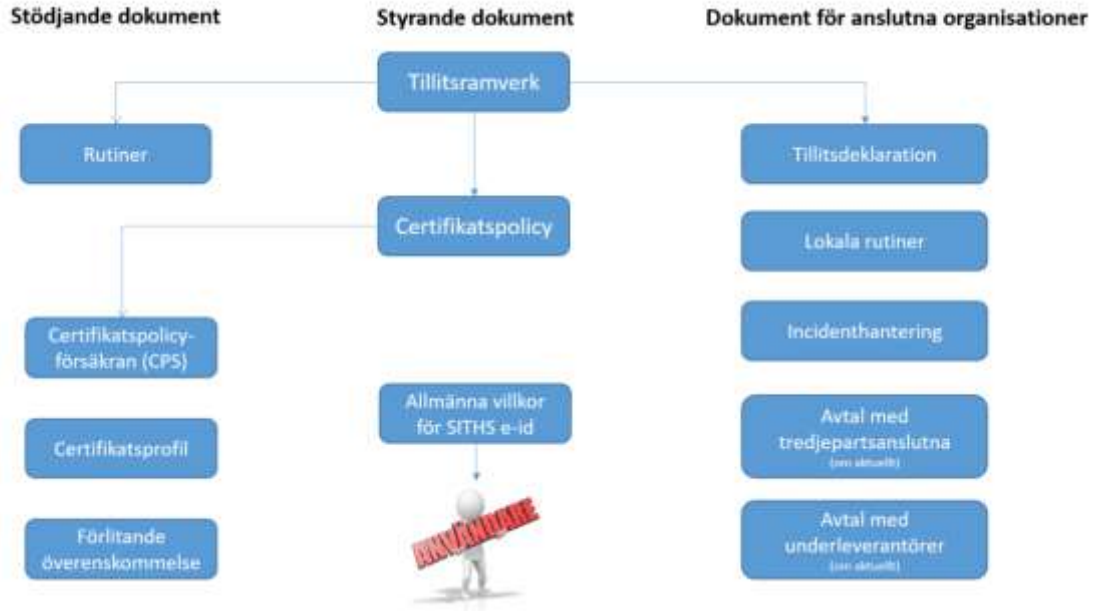
Regelverket för SITHS ägs och förvaltas av SITHS PA. Regelverket beskrivs i SITHS samlade dokumentstruktur. Varje organisation som direktansluter sig ska lämna in en tillitsdeklaration.

2.1.2 Förvaltning

Förvaltare av SITHS är Inera AB. Varje organisation som direktansluter sig för nyttjande av tjänsten ska teckna avtal med Inera AB.

2.2 SITHS övergripande dokumentstruktur

Alla styrande och stödjande dokument ägs och förvaltas av SITHS PA. Anslutningsdokument ägs av de anslutna organisationerna, men ska tas fram enligt mallar från SITHS PA. Lokala dokument ägs och formges av de anslutna organisationerna, i vissa fall har SITHS PA tagit fram exempeldokument som kan användas.



Figur 1 – SITHS övergripande dokumentstruktur. Överst i hierarkin finns SITHS Tillitsramverk

3. Säkerhet och Revision

SITHS PA har rätt att revidera alla anslutna organisationer. Vid sådan revision ska den anslutna organisationen skyndsamt vara behjälplig med framtagande av uppgifter och säkerställa att relevant personal finns tillgänglig.

3.1 Informationssäkerhet

Direktansluten organisation ska ha ett strukturerat säkerhetsarbete som ska omfatta:

a) en process för riskhantering som kontinuerligt analyserar hot och sårbarheter i verksamheten och bedömer sannolikhet och konsekvens för (skada på) användare, utgivningsområdet och andra anslutna organisationer inom SITHS. Resultatet från riskanalysen leder till säkerhetsåtgärder som ska balansera riskerna till acceptabla nivåer. Riskanalysen ska dokumenteras och kunna visas vid revision.
b) ett ledningssystem för informationssäkerhet eller funktion som motsvarar detta **Nivå 4** Ledningssystem för informationssäkerhet ska vara baserat på ISO/IEC 27001.
c) kontinuerligt genomförda och dokumenterade internrevisioner
d) en upprättad och testad kontinuitetsplan

3.2 Revision från SITHS PA

Direktansluten organisation kommer regelbundet att vara föremål för revision från SITHS PA. Revisionen kommer att genomföras enligt den vid varje tidpunkt gällande processen. De åtgärder som blir följd av revisionen ska genomföras av utgivningsområdet.

3.3 Internrevision

Direktansluten organisation ska minst var 13:e månad ha genomfört internrevision. Även utgivningsområdets tredjepartsanslutna ska omfattas av revision och under en treårsperiod ska samtliga tredjepartsanslutna ha blivit reviderade. Funna avvikelser ska resultera i en åtgärdsplan och denna ska genomföras. Internrevision och åtgärdsplan med genomförande ska dokumenteras.

Dokumentationen ska minst omfatta:

- Problem/risk/avvikelse
- Orsaker
- Förbättringsförslag
- Slutsats/rekommendation
- Mätning av effekt/nytta med förbättringsåtgärd från föregående internrevision

Genomförda internrevisioner ska kunna redovisas vid revision från SITHS PA.

Internrevision ska ledas av säkerhetsansvarig eller oberoende[2] kontrollfunktion.

3.4 Säkerhetsincidenter

Direktansluten organisation ska ha en dokumenterad och införd process för hantering av säkerhetsincidenter. Processen ska beskriva hur vidarerapportering till säkerhetsansvarig sker och när vidarerapportering till SITHS PA ska göras.

Vid säkerhetsincident ska lämpliga reaktiva och preventiva åtgärder vidtas för att lindra eller förhindra skada. Incidentrapport ska upprättas.

3.5 Spårbarhet, gallring och handlingars bevarande

Direktansluten organisation ska bevara de dokument som krävs. För att bistå den direktanslutna organisationen finns inom SITHS i flera fall elektroniska stöd framtagna och finns dessa ska de användas.

Dokumentation som ska bevaras:

a) godkänd tillitsdeklaration
b) förteckning av utsedda ID-administratörer samt deras områden, inklusive historik
c) avtal med tredjepartsorganisationer

[2] Oberoende innebär någon som inte är ID-administratör

d) kvittenser avseende utfärdade elektroniska identitetshandlingar
e) dokumentation av interna revisioner samt åtgärdsplaner
f) beställning av elektroniska identitetshandlingar för funktion och kvittens på mottagande

Tiden för bevarande ska inte understiga 10 (tio) år från skapandedatum och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallats ur integritetssynvinkel och har stöd i lag eller annan författning.

4. Direktansluten organisations förpliktelser

Varje direktansluten organisation ska utse en Ansvarig utgivare, en Säkerhetsansvarig samt upprätta en organisation för ansökan, beställning, utlämnande och support samt spärr av elektroniska identitetshandlingar för hela utgivningsområdet. Förändringar av Ansvarig utgivare, Säkerhetsansvarig och vilka organisationer som ingår i utgivningsområdet ska skyndsamt meddelas till SITHS PA.

Ansvarig utgivare ska ha tillräcklig tid och resurser avsatta för att klara sitt uppdrag.

4.1 Krav på Ansvarig utgivare och Säkerhetsansvarig

4.1.1 Personkontroller

Innan en person tilldelas rollen Ansvarig utgivare eller Säkerhetsansvarig ska en identitetskontroll med hjälp av godkänd id-handling ha genomförts.
Personerna får inte ha annat uppdrag som kan bedömas stå i konflikt med arbetet inom utgivningsområdet.

För Ansvarig utgivare ska även en bakgrundskontroll enligt nedanstående ha gjorts.

Syftet med bakgrundskontrollen är att förvissa sig om att personen kan anses vara pålitlig och har de kvalifikationer och den utbildning som krävs för att på ett tillfredsställande, korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

Kontroller som ska utföras är:

- Nuvarande anställning
- Lämplighet för tjänsten
- Legal lämplighet
- Finansiell lämplighet
- Genomförd utbildning för Ansvarig utgivare respektive Säkerhetsansvarig

4.2 Ansvarig utgivares förpliktelser

Ansvarig utgivare:

- har det övergripande ansvaret för att upprätta ett utgivningsområde med tillräckliga personella resurser för att uppfylla organisationens åtaganden

- ansvarar för att utgivningsområdet följer SITHS regler och rutiner om ansökan, beställning, utlämnande och spärr av elektroniska identitetshandlingar till personer och funktioner
- ansvarar för att personkontroller utförs på alla personer som är ID-administratörer inom utgivningsområdet
- ansvarar för att ID-administratörer har adekvat kunskap och kompetens för att upprätthålla organisationens åtagande

4.2.1 Personkontroller av ID-administratörer

Innan en person tilldelas en roll inom utgivningsområdet ska Ansvarig utgivare, eller en områdesansvarig som denna delegerat ansvaret till, ha genomfört en identitetskontroll med hjälp av godkänd id-handling samt gjort en bakgrundskontroll. Syftet med bakgrundskontrollen är att förvissa sig om att personen kan anses vara pålitlig och har de kvalifikationer och den utbildning som krävs för att på ett tillfredsställande, korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

Personen får inte ha annat uppdrag som kan bedömas stå i konflikt med arbetet inom utgivningsområdet.

Rutiner för kontroller och vilka kontroller Ansvarig utgivare väljer att göra ska beskrivas i tillitsdeklarationen och ska godkännas av SITHS PA. Minst tre olika kontroller ska genomföras per ID-administratör.

Exempel på kontroller som kan utföras är:

- Kontroll av nuvarande anställning
- Intyg på lämplighet för tjänsten
- Genomförd relevant utbildning
- Utdrag ur belastningsregistret

4.2.2 Utbildning av ID-administratörer

Alla ID-administratörer ska ha adekvat kunskap och förmåga. Ansvarig utgivare ska tillse att deras kunskap upprätthålls så att de kan fullgöra sina arbetsuppgifter på ett sådant sätt att tilliten säkras. Uppföljning av utbildning av administratörer ska genomföras så att kvalité upprätthålls inom utgivningsområdet.

4.3 Säkerhetsansvarigs förpliktelser

En Säkerhetsansvarig ansvarar för att utvärdera utgivningsområdets efterlevnad av utgivningsprocesser för elektroniska identitetshandlingar. I detta ingår ansvar för att internrevisioner och riskanalyser genomförs samt tillsyn av Ansvarig utgivare.

Säkerhetsansvarigs roll får inte kombineras med annan roll inom utgivningsområdet.

Om Ansvarig utgivare lämnar rollen ska Säkerhetsansvarig skyndsamt tillse att en ny Ansvarig utgivare utses. Under tid som Ansvarig utgivare saknas övertar Säkerhetsansvarig temporärt de förpliktelser som normalt åligger Ansvarig utgivare, dock kan inte Säkerhetsansvarig få motsvarande behörigheter i systemen.

4.4 Krav på kontinuitetsplan

Inom varje utgivningsområde ska Ansvarig utgivare medverka till att det etableras och förvaltas kontinuitetsplaner med testade och dokumenterade rutiner. Rutinerna bör omfatta avbrottshantering för utgivning av elektroniska identitetshandlingar.

Respektive organisation ansvarar för möjlighet att komma åt centrala komponenter såsom spärrlistor. En kontinuitetsplan bör också omfatta åtgärder i samband med en externt uppkommen, allvarlig säkerhetsincident som till exempel innebär att SITHS inte går att använda.

5. Avveckling av utgivningsområde

En direktansluten organisation som vill avsluta sin anslutning till SITHS ska informera SITHS PA genom att säga upp sitt avtal. Andra organisationer som ingår i utgivningsområdet måste antingen ändra anslutning eller avslutas.

Den direktanslutna organisationen som står som ansvarig för tillitsdeklarationen ska:

a) informera alla användare och parter som organisationen har avtal eller överenskommelser med
b) avsluta avtal och behörigheter för utgivningsområdet
c) spärra alla elektroniska identitetshandlingar som är utfärdade inom utgivningsområdet
d) tillse att alla arkiv och loggar bevaras enligt gällande anvisningar i kapitel *Spårbarhet, gallring och handlingars bevarande*

6. Fysisk, administrativ och personorienterad säkerhet

6.1 Fysisk säkerhet

Nyckelmaterial och aktiveringsdata ska skyddas fysiskt mot skada och otillåten åtkomst.

Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till behörig personal. ID-administratörer ska ha exklusiv tillgång till låsbar förvaring för arkivmaterial och ännu inte uthämtade bärare.

6.2 Administrativ säkerhet

Åtkomst till SITHS Admin för ID-administratörer kräver identifiering med tillitsnivå 3.

6.2.1 Skydd av aktiveringsdata

Nivå 3

- Reservkort: vid personalisering skyddas aktiveringsdata genom flerpersonskontroll
- Ordinarie kort: aktiveringsdata distribueras via en från bäraren separerad kanal.

7. Elektroniska identitetshandlingar för Personer

7.1 Användningsområden

Elektroniska identitetshandlingar för personer utfärdade inom SITHS får användas med syfte att:

- Identifiera fysiska personer verksamma i offentlig sektor vid legitimering och underskrift

7.2 Information om villkor

Elektronisk identitet får lämnas ut först efter att användaren uppmärksammats på, och accepterat, villkoren för den elektroniska identiteten.

Användaren ska informeras om att förvara pin- och pukkoder och bärare så att obehöriga inte får tillgång till dessa samt att koder och bärare ska förvaras fysiskt åtskilda.

7.3 Ansökan

7.3.1 Förutsättningar

Elektroniska identitetshandlingar för personer kan tilldelas anställda inom utgivningsområdets organisationer eller till personer som utför uppdrag åt dessa.

Elektroniska identitetshandlingar får utfärdas endast på begäran av användaren eller genom annat likvärdigt acceptförfarande.

ID-administratör ska neka utfärdande om förutsättningarna inte är uppfyllda.

En ansökan om elektronisk identitet ska knytas till person-id eller HSA-id samt till de uppgifter som i övrigt är nödvändiga för att kunna tillhandahålla den elektroniska identiteten.

Nivå 2 Personen måste ha fyllt 15 år.

Nivå 2 Personen måste ha ett svenskt personnummer alternativt vid ett fysiskt besök visa upp ett pass eller nationellt id-kort som klarar granskning enligt gällande rutin.

Nivå 2

- Reservkort: Giltighetstiden för certifikatet får vara max 180 dagar.

Nivå 3 Personen måste ha fyllt 18 år.

Nivå 3 Personen måste ha ett svenskt personnummer och ha en folkbokföringsadress i Sverige.

Nivå 3

- Reservkort: Giltighetstiden för certifikatet får vara max 360 dagar.
- Ordinarie kort: Giltighetstiden för certifikatet får vara max 1830 dagar.

7.4 Beställning

7.4.1 Kontroll av uppgifter

ID-administratör ska kontrollera att uppgifterna knutna till ansökan är fullständiga och stämmer överens med uppgifter som finns registrerade i ett betrott register.

7.4.2 Identifiering vid beställning

All identifiering ska ske enligt av SITHS PA fastställda rutiner.

En identifiering kan göras i samband med beställning. Detta styrs av olika lokala regler eller krav från andra aktörer, till exempel DNV.

Nivå 2 krävs ingen identifiering av användaren.

Nivå 3 ska användaren redan vara identifierad genom en relation som rör ekonomiskt eller rättsligt betydelsefulla mellanhavanden. Utgivningsområdet bekräftar användarens uppgifter i ett betrott register.

Nivå 4 krävs identifiering och personlig närvaro av användaren.

7.5 Utlämning

Vid utlämning ska ID-administratören genomföra en identitetskontroll. Identifieringssättet ska dokumenteras.

7.5.1 Utlämning vid personligt besök

ID-administratören ska, vid personligt besök och efter utförd identitetskontroll, lämna ut den elektroniska identiteten mot undertecknad kvittens.

Nivå 2 Användaren ska underteckna en papperskvittens.

Nivå 3 Användaren ska kvittera den elektroniska identiteten med aktiveringsdata tillhandahållna separat och säkerhetsmässigt oberoende baserat på kontaktuppgifter förda i betrott register.

7.5.2 Utlämning på distans

Efter identifiering ska mottagande av den elektroniska identiteten kvitteras av användaren.

Nivå 2 Användaren ska underteckna en papperskvittens.

Nivå 3

- Utgivningsområdet som tillhandahåller elektronisk identitet på distans ska vid utgivning, notifiera användaren via en oberoende kanal om att elektronisk identitet har överlämnats, eller genom andra åtgärder säkerställa att användaren uppmärksammas på risken för identitetsstöld i samband med tillhandahållandet.
- Användaren ska kvittera den elektroniska identiteten med aktiveringsdata tillhandahållna separat och säkerhetsmässigt oberoende baserat på kontaktuppgifter förda i betrott register.

7.5.3 Identifiering vid utlämning

All identifiering ska ske enligt av SITHS PA fastställda rutiner.

Nivå 2

Identifiering av en användare sker vid ett personligt besök där användaren presenterar en giltig id-handling för en behörig ID-administratör.

Har användaren ingen giltig id-handling är även följande identifieringssätt godkända:

- Intygsgivning

I de fall ett personligt besök inte kan ske är även följande identifieringssätt godkända:

- En användare av en giltig elektronisk identitet utfärdad av SITHS intygar personlig vetskap om personens identitet genom en elektronisk signatur

Nivå 3

Identifiering av en användare sker vid ett personligt besök där användaren presenterar en giltig id-handling för en behörig ID-administratör.

I de fall ett personligt besök inte kan ske är även följande identifieringssätt godkända:

- Befintlig elektronisk identitet godkänd av SITHS PA
- Två användare av giltig elektronisk identitet utfärdad av SITHS intygar personlig vetskap om personens identitet genom en elektronisk signatur

Nivå 4

Identifiering av en användare sker vid ett personligt besök där användaren presenterar en giltig id-handling för en behörig ID-administratör.

7.6 Spärr

Spärrbegäran kan komma från användaren, verksamheten eller utgivande organisation.
Utgivningsområdet ska skyndsamt och på ett säkert sätt effektuera spärrbegäran.
Spärr kan utföras av användaren eller behörig ID-administratör.

Spärr görs om något av följande har inträffat:

- Förhållanden som kan påverka certifikatsinnehållet har ändrats
- Någon uppgift i den elektroniska identiteten är eller misstänks vara felaktig
- Användaren har tappat kontrollen över bäraren eller koderna
- När bärare återlämnas
- När användaren inte längre har någon koppling till utgivande organisation
- När den elektroniska identiteten inte längre behövs

8. Elektroniska identitetshandlingar för Funktioner

8.1 Användningsområden

Elektroniska identitetshandlingar för funktioner utfärdade inom SITHS får användas med syfte att:

- Identifiera IT-utrustning, tjänster, funktionsbrevlådor och andra objekt som inte är fysiska personer

8.2 Information om villkor

Funktionscertifikatsbeställare, tillika mottagare, utses enligt utgivningsområdets egna regler. Dessa ska beskrivas i tillitsdeklarationen. Elektronisk identitet för funktion får lämnas ut först efter att mottagaren uppmärksammats på, och accepterat, villkoren. Att villkoren accepterats ska arkiveras.

För att beställningen ska kunna genomföras måste domänen eller funktionen vara validerad av SITHS PA.

ID-administratören ska neka utfärdande om förutsättningarna inte är uppfyllda.

8.3 Ansökan

Ansökan ska knytas till domännamn, HSA-id eller annan unik identifiering samt de uppgifter som i övrigt är nödvändiga för att utgivande organisation ska kunna tillhandahålla den elektroniska identiteten.
Elektroniska identitetshandlingar inom SITHS får utfärdas endast på begäran av funktionscertifikatsbeställare. Varje utfärdande ska föregås av en ansökan, både vid förstagångsutfärdande och vid förnyelse.

8.4 Beställning

8.4.1 Kontroll av uppgifter

ID-administratören ska kontrollera att uppgifterna knutna till ansökan är fullständiga och stämmer överens med uppgifter som finns registrerade.

8.4.2 Identifiering

Funktionscertifikatsbeställaren identifieras enligt beskrivning i lokala rutiner.

8.5 Mottagande

Funktionscertifikatsbeställaren identifieras enligt beskrivning i lokala rutiner. En elektronisk kvittens eller en papperskvittens ska undertecknas och arkiveras.

8.6 Spärr

Spärrbegäran kan komma från funktionscertifikatsbeställare, verksamheten eller utgivande organisation.
Direktansluten organisation ska skyndsamt och på ett säkert sätt effektuera spärrbegäran.
Spärr kan utföras av behörig ID-administratör.

Spärr görs om något av följande har inträffat:

- Förhållanden som kan påverka certifikatsinnehållet har ändrats
- Någon uppgift i funktionens elektroniska identitet är eller misstänks vara felaktig
- Den privata nyckeln har röjts

- När funktionens elektroniska identitet inte längre behövs
- När utgivande organisation inte längre förfogar över domänen och en överenskommelse med den nya ägaren saknas

9. Regler för Ombud

För att agera ombud krävs en direktanslutning samt godkännande från SITHS PA.

9.1 Ansvarsfördelning

För ombud gäller hela tillitsramverket enligt ovan, nedanstående matris tydliggör relationen mellan ombud och tredjepart.

Uppgift/dokument	Ombud (Ansvarig utgivare)	Tredjepart	SITHS PA	Kommentar
Godkänner tredjepart	Ansöker	-	Beslutar	
Upprättar tredjepartsavtal	Ansvarig	Behjälplig	-	Följs upp vid revision
Initierar och ansvarar för att intern revision genomförs	Säkerhetsansvarig	Behjälplig	-	Se kapitlet om Internrevision
Svarar på extern revision samt tar fram och genomför åtgärder	Ansvarar och medverkar	Medverkar	Utför	Ombudet ansvarar för deltagande och att åtgärder genomförs enligt regelverket
Tillitsramverket	Ansvarar för efterlevnad	Efterlever	Äger	
Tar fram och inför lokala rutiner	Ansvarig	Efterlever	-	Lokala rutiner ska baseras på rutiner framtagna av SITHS PA i de fall sådana finns
Upprättar och uppdaterar tillitsdeklaration	Ansvarig	-	Godkänner	