Tillitsramverk för EFOS

Revisionshistorik

Version	Datum	Författare	Kommentar
1.0	2019-06-19	EFOS Policy Authority	Fastställd

Innehållsförteckning

1. Inledning

1.1 Bakgrund och syfte

E-identitet för offentlig sektor (EFOS) , är en tjänst tillhandahållen av Försäkringskassan som ska utfärda 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 EFOS. Tillämpningen av tillitsramverket beskrivs i de rutiner som fastställs av EFOS 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.

Kravuppfyllnad ska tolkas så att

a) om tillitsnivå inte anges ska kravet alltid uppfyllas, och
b) om tillitsnivå finns angiven, ska kravet uppfyllas på angiven nivå och alla överliggande.

1.2 Översikt

Detta dokument beskriver ramverket för EFOS som alla anslutna organisationer ska uppfylla. Tillitsramverket definierar grundkraven för EFOS Certifikatspolicy (EFOS CP) och tillsammans utgör de basen för alla övriga dokument som ingår i dokumenthierarkin. Se 2.2 för överblick.

Alla dokument finns på https://repository.efos.se/

1.3 Målgrupp

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

1.4 Identifiering

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

Namn för EFOS CP är:	{Swedish public sector x509 certificate policy}
Objektidentifierare (OID):	{1.2.752.146.200.2.0.0.6}
Namn på detta tillitsramverk är:	{Tillitsramverk för E-identitet inom offentlig sektor}
Objektidentifierare (OID):	{1.2.752.200.1.0.0.6}

[1] Exempel på bärare är kort och mobiltelefon

1.5 Begrepp

Se dokumentet ”Termer och begrepp för EFOS”.

2. Organisation och styrning

2.1 Övergripande krav

Organisation som vill ansluta sig till EFOS, 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 anslutit som tredjepart.

Varje direktansluten organisation ska ha en skriftlig överenskommelse med varje organisation som den har anslutit som tredjepart.

Undantag gällande tillitsramverket kan ske efter godkänd ansökan av EFOS PA.

2.1.1 Regelverk

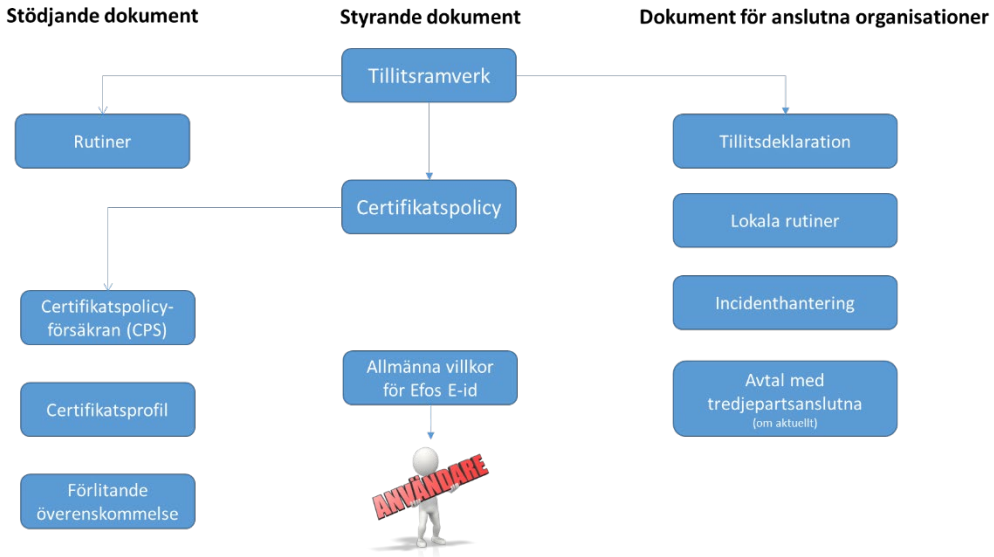
Regelverket för EFOS ägs och förvaltas av EFOS PA. Regelverket består av EFOS samlade dokumentstruktur. Varje organisation som direktansluter sig ska lämna in en tillitsdeklaration.

2.1.2 Förvaltning

Förvaltare av EFOS är Försäkringskassan.
Varje organisation som direktansluter sig för nyttjande av tjänsten ska teckna överenskommelse med Försäkringskassan.

2.2 EFOS övergripande dokumentstruktur

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



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

3. Säkerhet och Kontroll

EFOS PA har rätt att kontrollera alla anslutna organisationer och deras uppfyllnad av EFOS Tillitsramverk. Vid sådan kontroll 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 kopplade till EFOS och bedömer sannolikhet och konsekvens för (skada på) användare, organisationen och andra anslutna organisationer inom EFOS. Resultatet från riskanalysen leder till säkerhetsåtgärder som ska balansera riskerna till acceptabla nivåer.
Riskanalysen ska dokumenteras och kunna visas vid kontroll kopplad till tjänsten.
b) ett ledningssystem för informationssäkerhet eller funktion som motsvarar detta

c) kontinuerligt genomförda och dokumenterade egenkontroller för ingående organisationer
d) en upprättad och testad kontinuitetsplan

3.2 Kontroll från EFOS PA

Direktansluten organisation kommer regelbundet att vara föremål för kontroll från EFOS PA. Kontrollen kommer att genomföras enligt den vid varje tidpunkt gällande processen. De åtgärder som blir följd av kontrollen ska genomföras av organisationen.

3.3 Egenkontroll

Direktansluten organisation ska minst var 12:e månad ha genomfört egenkontroll. Försäkringskassan tillhandahåller mallar för egenkontrollen. Även tredjepartsanslutna ska omfattas av kontroll. Alla parter tar sina egna kostnader. Funna avvikelser ska resultera i en åtgärdsplan och denna ska genomföras. Egenkontroll och åtgärdsplan med genomförande ska dokumenteras.

Dokumentationen ska minst omfatta:

- Problem/risk/avvikelse
- Orsaker
- Förbättringsförslag
- Slutsats/rekommendation

Genomförda egenkontroller ska kunna redovisas vid revision från EFOS PA.

För Nivå 4 gäller att egenkontroll ska utföras av oberoende[2] intern kontrollfunktion.

3.4 Säkerhetsincidenter

Direktansluten organisation ska ha en dokumenterad och införd process för hantering av säkerhetsincidenter. Processen ska beskriva hur vidarerapportering sker och när vidarerapportering till EFOS PA ska göras. Vidarerapportering sker enligt beskrivning i ”SLA EFOS”

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

[2] Revision får inte ledas av någon som är ID-administratör

3.5 Spårbarhet, gallring och handlingars bevarande

Direktansluten organisation ska bevara de dokument som definieras nedan. För att bistå den direktanslutna organisationen finns inom EFOS 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, inklusive historik
c) avtal med tredjepartsorganisationer
d) kvittenser avseende utfärdade elektroniska identitetshandlingar
e) dokumentation av interna egenkontroller 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.

3.6 Fysisk säkerhet

3.6.1 Fysisk säkerhet

ID-administratörer ska ha exklusiv tillgång till låsbar förvaring för arkivmaterial och ännu inte uthämtade bärare (rekommenderad standard SS 3492 eller högre, läs mer PMFS 2019:2 3 kap. 10 §).

3.7 Administrativ säkerhet

Åtkomst till EFOS-portal för ID-administratörer kräver en överenskommelse mellan part och Försäkringskassan Efter tilldelning av rollen, som sker av ansluten part, krävs identifiering med tillitsnivå 3.

3.7.1 Skydd av aktiveringsdata

Nivå 3

- Tillfälliga kort: vid beställning av kort och certifikat med personlig information, skyddas aktiveringsdata genom flerpersonskontroll

- Ordinarie kort: aktiveringsdata distribueras via en från bäraren separerad kanal.

4. Direktansluten organisations förpliktelser

Varje direktansluten organisation ska utse en Ansvarig utgivare samt upprätta en organisation och process/rutin/riktlinje för ansökan, beställning, utlämnande och support samt spärr av elektroniska identitetshandlingar för respektive organisation. Förändringar av Ansvarig utgivare ska skyndsamt meddelas till EFOS PA.

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

4.1 Krav på Ansvarig utgivare

Personkontroller ska ske innan en person tilldelas rollen Ansvarig utgivare ska en identitetskontroll med hjälp av godkänd id-handling genomförts samt en säkerhetsprövning med registerkontroll lägst i klass 3 https://www.sakerhetspolisen.se/sakerhetsskydd/blanketter-och-informationsmaterial.html)

Syftet med säkerhetsprövning enligt ovan 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 inom organisationen som kan bedömas stå i konflikt med arbetet som ansvarig utgivare till exempel annan roll i administrationsverktyget.

4.1.1 Ansvarig utgivares förpliktelser

Ansvarig utgivare:

- har det övergripande ansvaret att organisationens uppfyller sitt åtagande enligt tillitsramverket
- ansvarar för att följa EFOS regler och rutiner om ansökan, beställning, utlämnande och spärr av elektroniska identitetshandlingar till personer och funktioner.
- säkerställer för att rutin finns för att personkontroller utförs på alla personer som är ID-administratörer inom organisationen.

4.2 Krav på EFOS Administratör

4.2.1 EFOS Administratör (EA) Personkontroller

Innan en person tilldelas rollen EA ska en identitetskontroll med hjälp av godkänd id-handling genomförts samt en säkerhetsprövning med registerkontroll lägst i klass 3 https://www.sakerhetspolisen.se/sakerhetsskydd/blanketter-och-informationsmaterial.html)

Syftet med säkerhetsprövning enligt ovan 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 inom organisationen som kan bedömas stå i konflikt med arbetet som EA.

4.2.2 EFOS Administratörs förpliktelser

Känna till och följa EFOS regelverk och organisationens interna regelverk och föreskrifter

- ansvarar för att ID-administratörer har adekvat kunskap och kompetens för att upprätthålla organisationens åtagande
- ansvarar för att tillse att egenkontroll och riskanalys genomförs

4.3 Krav på ID administratör

4.3.1 Definition ID-administratörer

ID-administratör är samlingsnamnet för operativa roller i utfärdandeprocesserna. Aktuella roller är EFOS Utfärdare (EU), EFOS Central Administratör (CA), EFOS Lokal Administratör (LA) och EFOS Lokal Administratör Tillfälligt kort (LATK), Rollerna har olika rättigheter som beskrivs i ”EFOS_Roller”.

4.3.2 Personkontroller av ID-administratörer

Innan en person tilldelas en roll som ID administratör inom organisationen ska en identitetskontroll ha genomförts med hjälp av godkänd id-handling samt gjort en säkerhetsprövning med registerkontroll lägst i säkerhetsklass 3, se https://www.sakerhetspolisen.se/sakerhetsskydd/blanketter-och-informationsmaterial.html

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

Rutiner för kontroller och vilka kontroller Ansvarig utgivare väljer att göra ska beskrivas i tillitsdeklarationen och ska godkännas av EFOS PA.

Exempel på kontroller som kan utföras är:

- Kontroll av nuvarande anställning
- Lämplighet för tjänsten

4.3.3 ID-administratörens förpliktelser

Känna till och följa EFOS regelverk och organisationens interna regelverk och föreskrifter.

4.3.4 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 kvalitet upprätthålls inom organisationen.

4.4 Krav på kontinuitetsplan

Inom varje organisation 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. MSB länk: https://www.msb.se/Upload/Produkter_tjanster/Publikationer/KBM/Kontinuitetsplanering%20-%20en%20introduktion.pdf

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 EFOS inte går att använda.

5. Avsluta anslutning

En direktansluten organisation som vill avsluta sin anslutning till EFOS ska, för att vara gällande, ske med 12 (tolv) månaders varsel ske skriftligen och vara undertecknad av behörig person. (Regleras ytterligare i Överenskommelsen mellan part och Försäkringskassan)

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 överenskommelse och behörigheter för organisationen.
c) spärra alla elektroniska identitetshandlingar som är utfärdade inom organisationen
d) tillse att alla arkiv och loggar bevaras enligt gällande anvisningar i kapitel *Spårbarhet, gallring och handlingars bevarande*

Regleras i överenskommelsen mellan Försäkringskassan och ansluten part.

6. Elektroniska identitetshandlingar för Personer

6.1 Användningsområden

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

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

6.2 Information om villkor

Användaren ska informeras om att förvara legitimeringskod, underskriftskod och upplåsningskod och enheter så att obehöriga inte får tillgång till dessa samt att koder och enheter ska förvaras fysiskt åtskilda.

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

6.3 Ansökan och beställning

Ansökan sker när en användare eller ansvarig chef initierar processen för utfärdande av certifikat enligt processen ”EFOS flöden”.

Beställning sker när en Id-administratör eller Funktionscertifikatsbeställare skickar iväg ordern efter att ha validerat ansökan.

6.3.1 Förutsättningar

Elektroniska identitetshandlingar för personer kan tilldelas anställda inom organisationen eller till personer som utför uppdrag åt denna.

Personpost med användardata måste finnas eller skapas i EFOS-portalen.

En ansökan om elektronisk identitet ska knytas till person-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 3 Personen måste ha fyllt 18 år, ha ett svenskt personnummer och ha en folkbokföringsadress i Sverige.

Nivå 4 Personen måste ha fyllt 18 år, ha ett svenskt personnummer och ha en folkbokföringsadress i Sverige.

Undantag från kravet på folkbokföringsadress ges om det gäller ett tillfälligt kort eller om personen har skyddad identitet.

6.3.2 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.

6.3.3 Identifiering

All identifiering ska ske enligt av EFOS PA fastställda rutiner.

En identifiering kan, utifrån nivå-krav, göras i samband med beställning. Detta styrs av olika lokala regler eller krav från andra aktörer, till exempel DNV(Det Norske Veritas).

Nivå 2 krävs ingen identifiering av användaren. Ansökan på distans kan genomföras utan identifiering av sökanden.

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

Nivå 4 krävs identifiering och personlig närvaro av användaren.

6.4 Utlämning

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

Elektroniska identitetshandlingar får utfärdas endast efter användarens godkännande av allmänna villkor.

6.4.1 Identifiering vid utlämning

All identifiering ska ske enligt av EFOS 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 av annan person i samma organisation

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

- En användare av en giltig elektronisk identitet utfärdad av EFOS 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 enligt de sju stegen(handboken De sju stegen med information för kontroll av identitet i svenska id-handlingar godkända av bankerna på uppdrag av Svenska Bankföreningen), för en behörig ID-administratör.

Nivå 4

Se nivå 3

6.4.2 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 kvittera den elektroniska identiteten digitalt

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

Nivå 4 Se nivå 3

6.5 Kontroll

Vid användandet av e-legitimation ska respektive myndighet och/eller system säkerställa att det vid verifieringen av innehavarens e-legitimation sker tillförlitliga kontroller av den elektroniska legitimationshandlingens äkthet och giltighet.

6.6 Spärr

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

Spärr ska göras 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

7. Elektroniska identitetshandlingar för Funktioner

7.1 Användningsområden

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

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

7.2 Information om villkor

Funktionscertifikatsbeställare, tillika mottagare, utses enligt organisationens 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 beställa måste domänen eller funktionen vara validerad av EFOS PA.

Funktionscertifikatsutfärdare ska neka utfärdande om förutsättningarna inte är uppfyllda.

7.3 Ansökan

Ansökan ska knytas till domännamn 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 EFOS får utfärdas endast på begäran av funktionscertifikatsbeställare.

7.4 Beställning

7.4.1 Kontroll av uppgifter

Interna certifikat: Funktionscertifikatsbeställaren ska kontrollera att uppgifterna knutna till ansökan är fullständiga och stämmer överens med uppgifter som finns registrerade.

Publika certifikat: Funktionscertifikatsbeställaren ska kontrollera att uppgifterna knutna till ansökan är fullständiga och stämmer överens med uppgifter som finns registrerade externt.

7.4.2 Identifiering

Funktionscertifikatsbeställaren identifieras genom sin elektroniska identitet.

7.5 Mottagande

Funktionscertifikatsbeställaren identifieras genom sin elektroniska identitet.

7.6 Spärr

Spärrbegäran kan komma från funktionscertifikatsbeställare, beställande organisation eller utgivande organisation.
Direktansluten organisation ska skyndsamt och på ett säkert sätt effektuera spärrbegäran.
Spärr kan utföras av funktionscertifikatsbeställare eller Portaladministratör.

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
- Den privata nyckeln har röjts
- När den elektroniska identiteten inte längre behövs
- När utgivande organisation inte längre förfogar över domänen och en överenskommelse med den nya ägaren saknas

8. Regler för Ombud

För att agera ombud krävs en direktanslutning samt godkännande från EFOS PA. Tredjepart är annan organisation som hanteras via ombud och är därför inte direktansluten till EFOS.

8.1 Ansvarsfördelning

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

Uppgift/dokument	Ombud (Ansvarig utgivare)	Tredjepart	EFOS PA	Kommentar
Godkänner tredjepart	Ansöker	-	Beslutar	
Upprättar tredjepartsavtal/överenskommelse	Ansvarig	Behjälplig	-	Följs upp vid kontroll
Initierar och genomför egenkontroll	Ansvarig	Behjälplig	-	Se kapitlet om Egenkontroll
Svarar på extern kontroll samt tar fram och genomför åtgärder	Ansvarar och medverkar	Medverkar	Initierar	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 EFOS PA i de fall sådana finns
Upprättar och uppdaterar tillitsdeklaration	Ansvarig	-	Godkänner	