Granskningsinstruktioner och checklista för Tillitsgranskare

Version: 2.0.1

Detta dokument ska användas av Sambis granskare vid deras granskning av Tillitsdeklaration gjorda enligt mallen ”Tillitsdeklaration version 2.0”. (Den mallen är i sin tur skriven för att användas med Sambi Tillitsramverk version 2.0.2).

Innehåll

Denna checklista gäller Tillitsdeklarationen för:

Namn organisation/företag

Organisationsnummer

Ange ett unikt versionsnummer för denna Tillitsdeklaration

Inledning

Denna instruktion som också är en checklista beskriver granskningens genomförande och hur resultatet avrapporteras. Instruktionen har i tillämpliga delar hämtat sin bas i standarderna ISO/IEC 27007:2017 och SS-EN ISO 19011:2017.

En Tillitsdeklaration ska visa hur en Sökande uppfyller de krav som anges i Sambi Bilaga 3 – Tillitsramverk. Dessa krav återfinns i detta dokument, där också granskaren ska checka av att hen har kontrollerat alla tillitskrav. Eventuella kommentarer anges i svarsrutor, som expanderar vid behov.

Utförande

Arbetet genomförs i form av dokumentgranskning av tillitsdeklaration med bifogade dokument. Dessa ska visa att Sökanden uppfyller Sambis Tillitsramverk i tillräckligt hög grad. Tillitsdeklarationen är en självdeklaration, och bifogade dokument är avsedda att styrka deklarantens påståenden i deklarationen.

Om det under granskningen inte är möjligt att enkelt fastställa granskningsslutsatser så kan granskaren ställa kompletterande frågor till kontaktpersonen för innehållet i tillitsdeklarationen. I det fall granskaren har skäl att tro att svar och påståenden inte på ett tillfredsställande sätt speglar verkligheten bör granskaren be om kompletterande information. I särskilda fall kan direkt kontakt, intervjuer och platsbesök förekomma. Eventuella kontakter ska dokumenteras i granskningens checklista.

När avvikelser från kravuppfyllnad dokumenteras bör följande ingå:

1. beskrivning av eller hänvisning till granskningskriterier,
2. beskrivning av avvikelse,
3. granskningsbelägg,
4. anknytande granskningsiakttagelser, om det är tillämpligt.

Dokumentgranskning

Granskarna ska bedöma om:

1. informationen i tillhandahållna dokument är

a) fullständig (allt förväntat innehåll finns i dokumentet),

b) korrekt (innehållet överensstämmer med andra pålitliga källor, t.ex. standarder, lagar och förordningar),

c) konsekvent (dokumentet är i sig självt konsekvent och med anknytande dokument),

d) aktuellt (innehållet är uppdaterat),

2. de dokument som granskas täcker kraven i tillitsramverket samt ger tillräcklig

information för att stödja att organisationens tillitsdeklaration uppfyller Sambis Tillitsramverk

Checklistans frågor anges med kursiv text.

Avrapportering

När de för granskningen utsedda Granskarna är överens om sin rekommendation, ska Tillitsadministratören informeras om detta via tillit@sambi.se. Tillitsadministratören kommer då att skapa ett användarkonto i systemet Sambi dokumenttransport. Därefter förväntas den Granskare som har utsetts som huvudgranskare att överföra deras ifyllda checklista för granskningen samt deras slutgiltiga rekommendation till Tillitsadministratören. Denna överföring ska ske via systemet Sambi dokumenttransport.

Allmänt

Omfattning

Granskare av tillitsdeklaration

Ange namn, telefon, e-post för samtliga granskare

Namn på granskad organisation

Organisationsnummer för granskad organisation

Referens till tillitsdeklarationen

Ange datum eller versionsnummer.

Personer som har kontaktats för att klargöra eventuella frågor under granskningen av denna tillitsdeklaration

Ange namn, telefon, e-post, datum för kontakten och ärende för varje tillfälle.

Tillitsdeklarationens omfattning

Är omfattningen tydligt angiven, inkluderande Funktion, del av organisation och roller?

A. Generella krav

Övergripande krav på verksamheten

Krav A.1

Betrodd Part som inte är ett offentligt organ ska drivas som registrerad juridisk person samt teckna och vidmakthålla för verksamheten erforderliga försäkringar.

Är organisationsform och ägarförhållande tillfredsställande beskrivet?

Är försäkringar, och omfattning av dessa, tillfredställande beskrivet om Sökanden inte är ett Offentligt organ?

Krav A.2

Betrodd Part ska ha en etablerad verksamhet och vara fullt operationell i alla delar som berörs i detta dokument.

Har Sökanden visat att verksamheten är fullt operationell i berörda delar?

Är bevakning av befintliga och nya legala krav tillfredsställande beskrivet?

Säkerhetsarbete

Krav A.3

Betrodd Part ska för den funktion som medlemskapet avser ha infört ett strukturerat säkerhetsarbete anpassat efter risker och säkerhetsbehov, bestående av:

(a) En **riskanalys** avseende funktionen. Denna ska ta hänsyn till skyddsvärde, befintliga skyddsåtgärder och legala krav. Riskanalysen ska omfatta analys av hot och sårbarheter, samt sannolikhet och konsekvens (skada) på Användare, den egna organisationen, andra Medlemmar och Federationsoperatören.
(b) Ett **ledningssystem för informationssäkerhet** för funktionen baserat på ISO/IEC 27001 eller motsvarande. Säkerhetsåtgärderna ska hantera riskerna enligt riskanalysen för funktionen.
(c) Genomförd **internrevision** av införandet och efterlevnaden av säkerhetsregelverket för funktionen.

Riskanalys och internrevision ska genomföras årligen och leda till en förbättringsplan

innehållande rekommenderade säkerhetsåtgärder.

Har Sökanden beskrivit planering, periodicitet, fastställande av kontext, riskbedömning och riskidentifiering, riskbehandling, riskkommunikation och hur säkerhetsregelverket uppdateras för riskanalyser?

Granskaren ska beakta

- *Har en riskanalys genomförts?*
- *Stämmer inriktningen och omfattningen på riskanalysen med den aktuella funktionen?*
- *Har riskanalysen resulterat i en åtgärdsplan?*

Granskaren ska beakta:

- *Är ledningssystemet tillfredsställande beskrivet?*
- *Följer ledningssystemet för informationssäkerhet ISO 27001? Detta är inte ett krav enligt Sambi, men underlättar bedömningen för granskaren.*
- *Omfattar ledningssystemet den aktuella funktionen?*
- *Är ledningssystemet fastställt och infört?*
- *Har betrodd Part ett certifierat ledningssystem för informationssäkerhet och är den tillämplig på omfattningen av organisationens tillitsdeklaration? Detta är inte ett krav enligt Sambi, men underlättar bedömningen för granskaren.*
- *Finns i så fall en kopia av detta certifikat bifogat ansökan, och är certifikatet giltigt?*

Är genomförande, rapportering och hantering av avvikelser/förbättringsförslag tillfredsställande beskrivet för internrevisioner?

Är beslut, prioritering, resurs- och tidsättning, genomförande och uppföljning tillfredsställande beskrivet för förbättringsplanen?

Visar organisationen att den följer sitt ledningssystem för informationssäkerhet?

Visar organisationen att den har tillräckligt hög säkerhetsnivå för att övriga Medlemmar ska kunna ha tillit till denna? Detta är den viktigaste, sammanfattande, bedömningen för granskaren att göra. Granskaren ska här väga samman styrkor och svagheter i svaren ovan.

Krav A.4

Betrodd Part ska tillhandahålla dokumentation över genomförd riskanalys, ledningssystemet för informationssäkerhet samt genomförd internrevision av efterlevnaden och införandet av säkerhetsregelverket, inklusive aktuell förbättringsplan, avseende Ffunktionen.

Granskaren ska avgöra om bifogade dokument visar att krav A.3 är uppfyllt. Det kan exempelvis innebära granskning av att:

- *Relevanta skyddsåtgärder enligt ISO 27001, eller motsvarande, omfattas genom att relevanta delar pekas ut av riskanalys, internrevision, lagkrav eller "best practice".*
- *Riskanalysen är aktuell.*
- *Motivering för att inte tillämpa skyddsåtgärder är tillfredsställande beskrivet.*
- *Internrevisionen visar hur säkerhetsregelverket följs*

Stödfrågor:

Finns riskanalyser och internrevisioner bifogade med ansökan, så att det går att se att hela tillitsramverket och vilka delar av ISO 27001 som omfattas? Är riskanalysen aktuell? Är motiveringen när risker inte hanterats tillfredsställande beskrivet?

Har Sökanden bifogad aktuell förbättringsplan? Har ledningens genomgång av denna haft inflytande på förbättringsplanen? Har incidenter påverkat förbättringsplanen?

Har Sökanden bifogat dokumentation som beskriver ledningssystemet i tillräcklig omfattning?

Krav A.5

Medlem ska inrätta en process för incidenthantering som innefattar vidarerapportering till Federationsoperatören i enlighet med de av Federationsoperatören angivna instruktionerna.

Är incidenthanteringsprocessen tillfredsställande beskrivet? Inkluderar processen korrigerande och förebyggande åtgärder som resultat av incidenter?

Granskning och uppföljning

Krav A.6

Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs på Betrodd Part ska under en treårsperiod vara föremål för internrevision, utförd av oberoende kontrollfunktion.

Sambi granskningsgrupp ska genomföra en Tillitsgranskning vid ansökan och därefter minst var tredje år enligt Bilaga 4 - Föreskrifter för Sambis Federationsoperatör. Ett Sambiombud ska granskas årligen enligt Bilaga 5 av Sambiombudsavtalet.

Har kravet på en treårsperiod följts så att helheten täcks under periodens internrevisioner? Är Internrevision utförd av en extern part eller annan, oberoende, del av den egna organisationen som kan vara ”har en annan chef”?

Har det gått mer än tre år sedan föregående tillitsdeklaration upprättades?

Är planeringen, periodiciteten, omfattningen, hur revisorn utses och hur kvalitén säkras tillfredsställande beskrivet för internrevisionerna?

Kryptografisk säkerhet

Krav A.7

Betrodd Part ska skydda kryptografiskt nyckelmaterial, omfattande minst signeringsnycklar för

a) metadata
b) identitetsintyg
c) kommunikation

Krav på nyckelhantering ges i Bilaga 2, Tekniska krav.

Har Sökanden beskrivit hur de tekniska kraven uppfylls?

Ansvar för användning av Underleverantörer

Krav A.8

Betrodd part som lägger ut utförande av funktion på Underleverantör är som huvudman ansvarig för Underleverantörens uppfyllande av kraven i Tillitsramverket, oavsett avtalsform, och ska redogöra för hur Underleverantören uppfyller kraven så som om det vore utfört av den Betrodde Parten själv. I denna redogörelse ska Betrodd Part bl.a.

redovisa:

(a) hur Underleverantören uppfyller kraven i Tillitsramverket
(b) vilka funktioner och kritiska processer som har lagts ut på Underleverantör och hur Betrodd Part säkerställer att Underleverantören uppfyller kraven för dessa
(c) de avtal som definierar vilka funktioner som har lagts ut, hur kraven uppfylls av Underleverantören samt hur uppföljningen utförs.

A.8.a Har Sökanden beskrivit hur Leverantörer uppfyller samtliga krav i Tillitsramverket? Dessa svar kan ges vid respektive krav i tillitsdeklarationen. Svaren förenklas väsentligt om Leverantörer redan är granskade och godkända av Sambi.

Är speciellt det centrala kravet A.4, där riskanalys ska göras hos respektive Leverantör, ett ledningssystem ska finnas och internrevision ska göras tillfredsställande beskrivet för varje Leverantör?

A.8.b Har Sökanden tydligt redovisat om det är den egna organisationen eller en underleverantör som utför säkerhetsåtgärder?

Har Leverantören ett ledningssystem för informationssäkerhet och är det tillämpligt på omfattningen av organisationens tillitsdeklaration? Har Sökanden bifogat en kopia av leverantörens certifikat och är certifikat giltigt? Detta är inte ett krav enligt Sambi, men underlättar granskningen.

A.8.c Är de Funktioner och kritiska processer som lagts ut på Leverantörer tillfredsställandebeskrivna? Är kontroll av att Leverantören uppfyller kraven för dessa tillfredsställande beskrivet?

Är de egna rutinerna för att följa upp leverantören tillfredsställande beskrivna?

Handlingars bevarande

Krav A.9

Betrodd Part ska, i tillämpliga delar, bevara

(a) avtal
(b) styrande dokument

(c) handlingar som rör förändringar av uppgifter hänförliga till Användare, Attribut och Metadata och
(d) övrig dokumentation som stöder efterlevnaden av de krav som ställs på denne, och som visar att de säkerhetskritiska processerna och kontrollerna fungerar.

Är detta bekräftat?

Är listan fullständig över allt material som ska arkiveras? Är all information som följer av organisationens tillämpning av ISO 27001 med i listan?

Är identifiering och arkivering av sådant material tillfredsställande beskrivet?

Krav A.10

Tiden för bevarande ska inte understiga tre år och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt och har stöd i lag eller annan författning.

Har Sökanden beskrivit hur material enligt A.9 kan tas fram och läsas? Har Sökanden redovisat om avvikelse sker från angiven tid enligt krav A.10, och är motivet i sådana fall detta tillfredsställande beskrivet?

Information

Krav A.11

Betrodd Part ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av funktionen till Användare, Tjänsteleverantörer och andra som kan komma att förlita sig på denne.

Är krav A.11 bekräftat och har Sökanden tillfredsställande beskrivit hur dessa uppgifter tillhandahålls?

Krav A.12

Betrodd Part ska till Federationsoperatören tillhandahålla en Tillitsdeklaration som beskriver hur Betrodd Part uppfyller Tillitsramverket. Dokumentet ska följa av Federationsoperatören angivet format. Till denna ska bifogas efterfrågade dokument enligt detta Tillitsramverk.

Har den Sökande tillhandahållit en Tillitsdeklaration i rätt version och format? Har alla efterfrågade dokument bifogats?

Krav A.13

Betrodd Part ska på begäran av Federationsoperatören lämna uppgifter om hur verksamheten ägs och styrs.

Är detta bekräftat?

Krav A.14

Betrodd Part ska på ett tydligt sätt informera sina Användare och Federationsoperatören om villkor för funktionen vid nyteckning eller ändring av funktionen. Betrodd Part ska informera Federationsoperatören även vid ändringar av kontaktpersoner, federationsgemensamma Metadata och Attribut.

Är detta bekräftat och är tillvägagångssättet för att aktivt informera användarna om villkoren vid nyteckning eller ändring av tjänsten tillfredsställande beskrivet?

Krav A.15

En Betrodd Part som upphör med sin verksamhet ska informera berörda Användare, Betrodda Parter och Federationsoperatören. Den Betrodda Parten ska hålla arkiverat material tillgängligt i enlighet med A.9 och A.10.

Är detta bekräftat och är förberedelser för detta tillfredsställande beskrivet?

B. E-legitimationsutfärdare

Krav B.1

E-legitimationsutfärdare ska vara godkänd av E-legitimationsnämnden som Utfärdare av Svensk e-legitimation på tillitsnivå 3 i enlighet med

E-legitimationsnämndens Tillitsramverk.

Har Sökanden bekräftat att detta har skett och har godkännande från E-legitimationsnämnden bifogats?

C. Attribututgivare

Krav C.1

Informationsinnehållet i Attribut ska vara korrekt, aktuellt samt verifierat mot ursprungskällan.

Har Sökanden tagit hänsyn till resultatet av riskanalysen avseende vilka attribut som är viktigast ur säkerhetssynpunkt? Har Sökanden beskrivit

- *hur han säkerställer att attribut är korrekta?*
- *hur attribut hålls aktuella över tiden?*
- *hur verifiering görs?*

Krav C.2

Förändringar av informationsinnehållet i Attribut ska gå att spåra avseende tidpunkt för förändring och vem som utfört förändringen.

Har Sökanden beskrivit hur loggning görs, vilket innehåll loggarna har, regler och rutiner (ansvar) för uppföljning av innehållet i loggar, samt hur loggarna säkras från otillbörlig manipulering?

D. Identitetsintygsutgivare

Krav D.1

Betrodd Part som tillhandahåller tjänst för utgivning av Identitetsintyg ska se till att denna tjänst har god tillgänglighet och att utlämnande av Identitetsintyg föregås av en tillförlitlig kontroll av att den angivna Användarens Elektroniska identitet och Attribut är giltiga.

Är ett tillförlitlighetsmått för tjänsten tillfredsställande beskrivet? Är kontroll av identitet och attribut, inklusive vilka attributskällor som används, tillfredsställande beskrivet?

Krav D.2

Lämnade Identitetsintyg ska vara giltiga endast så länge som det krävs för att Användaren ska få tillgång till den efterfrågade E-tjänsten.

Är giltighetstid för intyg tillfredsställande beskrivet?

Krav D.3

Identitetsintyg ska skyddas så att informationen endast är läsbar för den mottagande Tjänsteleverantören och att denne kan kontrollera att mottagna intyg är äkta.

Är krypterings- och signeringsförfarande tillfredsställande beskrivet?

Krav D.4

Identifierade Användares anslutningar mot intygsutgivningstjänsten ska tidsbegränsas, varefter en ny identifiering av Användaren ska ske i enlighet med D.1.

Är tiden som en autentisering är giltig mot intygsutfärdaren tillfredsställande beskrivet?

E. Tjänsteleverantör

Krav E.1

Tjänsteleverantör ska ha en dokumenterad rutin för att publicera aktuella Attribut och Tillitsnivåer som används för Tjänstens behörighetskontroll.

Är denna rutin tilfredsställande beskriven? Är styrning av åtkomst och behörighet med angivande av regler och värden till tjänsten tillfredsställande beskrivet?

Krav E.2

Tjänsteleverantör ska skydda Användares identitet och tillhörande Attribut.

Har Sökanden bekräftat att detta sker? Är skydd av identiteter och Attribut för Användare tillfredsställande beskrivet?

Krav E.3

Tjänsteleverantör ska informera Användare om informationen sprids eller används på annat sätt än för behörighetsstyrning.

Har Sökanden bekräftat att detta sker? Är metod för information om hur sådan informationsspridning, intygspropageringn eller användning görs, och till vem, tillfredsställande beskrivet? Är det tillfredställande beskrivet hur Användaren informeras om detta?

F. Sambiombud

Övergripande krav på verksamheten

F.1 Sambiombud ska ha förmåga att bära risken för skadeståndsskyldighet samt förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst 1 år.

Har Sökanden beskrivit hur finansiering och försäkringar gör att detta krav är uppfyllt? Observera att frågan normalt inte behöver besvaras av ett offentligt organ.

Tillitsgranskning av anslutna Användarorganisationer

F.2 Sambiombudet ska ha väl dokumenterade rutiner för att säkerställa att anslutna Användarorganisationer uppfyller Tillitsramverket, samt att aktuella Tillitsdeklarationer finns för samtliga Användarorganisationer. Dessa rutiner skall minst omfatta kraven i ”Bilaga 5, Föreskrifter för Sambiombud”, till Sambiombudsavtalet. Sambiombudet ska kunna visa att dessa rutiner tillämpas och efterlevs.

Hänsyn ska tas till att Användarorganisationen nyttjar Sambiombudets tjänster för E-legitimationsutfärdande, attributhantering och intygsutgivning och därmed följande minskning av de återstående riskerna hos Användarorganisationen.

Om Användarorganisationen för sin kravuppfyllnad använder ytterligare riktlinjer utfärdade från Sambiombudet skall denne säkerställa att dessa följs och uppfylls.

Har Sökanden bifogat beskrivningar över samtliga rutiner enligt Bilaga 5 till Anslutningsavtalet? Har Sökanden visat att dessa rutiner är införda och följs? Rutinerna ska minst omfatta:

- *Hjälp att upprätta Användarorganisationers Tillitsdeklaration*
- *Rutin för leverans av Tillitsdeklaration från Användarorganisation med tillräcklig konfidentialitet*
- *Rutin för adminstration av Tillitsdeklarationer från Användarorganisationer*
- *Rutin för kontroll av efterlevnad av Tillitsramverket av Användarorganisationen i vissa fall*
- *Rutin för administration av Användarorganisationers kontaktuppgifter, inkluderande registerhållning och kommunikation till Federationsoperatören*
- *Rutin för kontroll av Användarorganisationer vid ansökan minst avseende behörighet som Sambimedlem och att signering gjorts av fimatecknare eller annan behörig person*
- *Rutin för lagring av Anslutningsavtal och arkivering i 10 år*

- *Rutin för kommunikation med Användarorganisationer*

- *Rutin för uppdatera, spärra, ta bort och kommunicera Metadata till Federationsoperatören*

Incidenthantering

F.3 Sambiombudet ska ha väl dokumenterade rutiner för hantering av incidenter i den egna verksamheten och hos sina Användarorganisationer. Dessa ska minst omfatta att:

- informera Federationsoperatören om det inträffade,
- vidta åtgärder för att återställa förtroende, och
- bistå Medlemmen i dess arbete att återskapa förtroendet för Elektroniska identiteter och Attribut i Sambi.

Har Sökanden bifogat beskrivningar över hantering av Incidenter hos Ombudet och dess anslutna Användarorganisationer? Dessa rutiner ska omfatta information till Federationsoperatören, åtgärder för att återställa förtroende samt bistånd till anslutna Användarorganisationer samt hjälp för tillfällig spärr av Metadata.

Har Sökanden krishanteringsrutiner och krisorganisation inklusive aktuella kontaktuppgifter.

Har Sökanden visat att dessa rutiner följs?