Checklista för Tillitsgranskare

Version: 2.1

Detta dokument ska användas av Sambis granskare vid deras granskning av Tillitsdeklaration gjorda enligt mallen ”Tillitsdeklaration version 2.1”. Mallen är skriven för att användas med Sambi Tillitsramverk version 2.1.

Innehåll

Denna checklista gäller Tillitsdeklaration för:

Namn organisation/företag

Organisationsnummer

Ange ett unikt versionsnummer för denna Tillitsdeklaration

Inledning

Denna 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, via Internetstiftelsen, ställa kompletterande frågor till kontaktpersonen om 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?

Avser ansökan Gruppföreträdare? Finns bilaga som beskriver kravuppfyllnad mot Bilaga 5 – Föreskrifter för Gruppföreträdare med och har acceptabelt innehåll? Avser ansökan Sambiombud?

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 Tillitsdeklarationen avser ha infört ett strukturerat säkerhetsarbete anpassat efter risker och säkerhetsbehov i enlighet med Tillitsramverket.

Beskrivning av den sökandes strukturerade säkerhetsarbete.

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? Är ansvaret över initiering och uppföljning tydligt definierat?*
- *Stämmer inriktningen och omfattningen på riskanalysen med den aktuella funktionen?*

- *Har riskanalysen resulterat i en åtgärdsplan?*

Granskaren ska beakta:

- *Är ledningssystemet tillfredsställande beskrivet? Är ansvaret för Ledningssystemet definierat?*
- *Följer ledningssystemet för informationssäkerhet ISO 27001?*
- *Omfattar ledningssystemet den aktuella funktionen?*
- *Är ledningssystemet fastställt och infört?*

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.

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 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 Funktionen 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? Om inte så kan det vara aktuellt att be om att få dokument med sekretesskänsligt innehåll uppvisade.

Krav A.4

Betrodd part har inrättat en process för incidenthantering i enlighet med de av Federationsoperatören angivna instruktionerna.

Är incidenthanteringsprocessen tillfredsställande beskriven? Inkluderar processen uppföljning av incidenter, samt korrigerande och förebyggande åtgärder som resultat av incidenter?

Kryptografisk säkerhet och skydd mot obehörig åtkomst

Krav A.5

Betrodd Part ska skydda Funktionen mot obehörig åtkomst.

Krav på skydd och nyckelhantering finns i Bilaga 2, Tekniska krav.

Är funktionen tillräckligt skyddad mot obehörig åtkomst?

Är det kryptografiska skyddet tillräckligt beskrivet? Finns det identifierbara brister i det kryptografiska skyddet?

Ansvar för användning av Underleverantörer

Granskning och uppföljning

Krav A.6

Betrodd part som, i delar eller i helhet, lägger ut utförande av Funktionen på Underleverantör är, oavsett avtalsform, ansvarig för Underleverantörens uppfyllande av kraven i Tillitsramverket.

Beskriv vilka delar av Funktionen som är utlagda till Underleverantörer och beskriv avtalsförhållandena.

Är det tillräckligt beskrivet vilka delar som hanteras av underleverantör?

Är det beskrivet hur underleverantören uppfyller villkoren i Tillitsramverket?

Är det tillräckligt beskrivet hur den sökande följer upp följsamheten hos underleverantörerna?

Är det reglerat i avtal att underleverantören ska följa Tillitsramverket eller hur är det reglerat?

Detta krav anger att tilliten inom Sambi ska vara oberoende av om organisationen använder sig av Underleverantörer eller utför i egen regi. Samtliga krav ska uppfyllas och redovisas oavsett var tjänsten eller funktionen utförs. Ifall Underleverantörer används ska det för samtliga krav redovisas hur Underleverantörerna uppfyller dem.

Detta gäller speciellt det centrala kravet A.3, där riskanalys ska göras hos respektive Underleverantör, ett ledningssystem ska finnas och internrevision ska göras.

Detta krav påverkar således hur samtliga övriga krav ska besvaras.

Beskriv hur eventuella Underleverantörer uppfyller kraven, i den mån detta inte redovisas under respektive krav. När Underleverantören har ett certifierat ledningssystem för informationssäkerhet, bifoga även kopia av Underleverantörens certifikat. Om Underleverantören är en Betrodd Part räcker detta för att visa att kravet är uppfyllt.

Ange de funktioner och kritiska processer som lagts ut på Underleverantörer. Beskriv hur kontroll sker att Underleverantören uppfyller kraven för dessa.

Ange vilka avtal som reglerar utförandet hos Underleverantören och beskriv hur dessa säkerställer att kraven uppfylls. Beskriv även de egna rutinerna för att följa upp Underleverantören.

Handlingars bevarande

Krav A.7

Betrodd Part ska, i tillämpliga delar, bevara

(a) avtal *som rör Funktionen*
(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 det tillräckligt beskrivet hur material identifieras och arkiveras?

Krav A.8

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.

Är det tillräckligt beskrivet hur det säkerställs att listat material kan tas fram och läsas? Är eventuella avvikelser försvarbara?

B. E-legitimationsutfärdare

Krav B.1

E-legitimationsutfärdare ska vara godkänd av Myndigheten för digital förvaltning (DIGG) i enlighet med Tillitsramverket för Svensk e-legitimation eller vara anmäld av annat land enligt EU:s eIDAS-förordning. Dessutom är SITHS godkänt i Sambi fram till 2020-06-30 även utan DIGG:s godkännande.

Är de angivna e-legitimationen godkända av Myndigheten för digital förvaltning (DIGG), godkända enligt eIDAS, eller är det SITHS? Ange eventuella avvikelser eller frågetecken.

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 tillgänglighetsmått för tjänsten tillfredsställande beskrivet? Är kontroll av identitet och attribut, inklusive vilka attributskällor som används, tillfredsställande beskrivet? Har de angivit kopplingen från identitetsintygstjänsten till godkända e-legitimationer?

Krav D.2

Tillitsnivå ska anges i identitetsintyget. Hur Tillitsnivå anger och tolkas ska följa specifikation från Myndigheten för digital förvaltning (DIGG).

Vilka tillitsnivåer är aktuella?

Krav D.3

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

Finns en kortvarig giltighetstid för intyg angiven?

Krav D.4

Informationen i identitetsintyg ska skyddas mot obehörig åtkomst.

Är krypteringsförfarandet beskrivet på ett tillfredsställande sätt?

Krav D.5

Identitetsintyg ska utfärdas på ett sådant sätt så att Tjänsteleverantören kan kontrollera att mottagna intyg är äkta.

Är signeringsförfarandet beskrivet på ett tillfredsställande sätt?

Krav D.6

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

Hur länge är autentiseringen mot intygsutfärdaren giltig innan ny autentisering krävs? Är längden acceptabel?

E. Tjänsteleverantör

Krav E.1

Tjänsteleverantör ska ha en dokumenterad rutin för publicering av Attribut och Tillitsnivåer som används för Tjänstens behörighetskontroll.

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

En Användarorganisation måste få information om vilka egenskaper deras Användare ska ha för att få åtkomst till hela eller delar av tjänsten. Detta ska återspeglas i krav på kvalité och aktualitet på nödvändiga Attribut.

Beskriv hur åtkomst och behörighet styrs till erbjuden tjänst med angivande av regler och värden.

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?

Bekräfta och beskriv hur skydd av identiteter och Attribut för Användare sker.

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, intygspropagering eller användning görs, och till vem, tillfredsställande beskrivet? Är det tillfredställande beskrivet hur Användaren informeras om detta?

Beskriv om sådan informationsspridning, intygspropagering eller användning görs, och till vem. Beskriv i så fall hur Användaren informeras om detta.

F. Sambiombud

Övergripande krav på verksamheten

F.1 Sambiombud ska ha erforderliga försäkringar samt förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten vidare 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.

Beskriv kortfattat hur finansiering och exempelvis försäkringar gör att kravet uppfylls. Notera att detta är en utvidgning av krav A.1. För ett offentligt organ behöver denna fråga normalt inte besvaras.

Tillitsgranskning av anslutna Användarorganisationer

F.2 Sambiombudet ska ha väl dokumenterade rutiner för att säkerställa att anslutna Användarorganisationer uppfyller kraven i kapitel A ”Generella krav” av detta ramverk.

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

Om Användarorganisationen för sin kravuppfyllnad använder riktlinjer utfärdade av 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 administration 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 firmatecknare eller annan behörig person

- *Rutin för lagring av Anslutningsavtal och arkivering i 10 år*
- *Rutin för kommunikation med Användarorganisationer*
- *Rutin för att uppdatera, spärra, ta bort och kommunicera Metadata till Federationsoperatören*

F.3 Sambiombudet ska ha väl dokumenterade rutiner för att tillse att en aktuell Tillitsgranskning finns för Användarorganisationer.

Finns dokumenterade rutiner?

Beskriv och bifoga dessa rutiner. Bifoga också en sammanställning av utfallet av användningen av rutinerna.

Incidenthantering

F.4 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?

Beskriv och bifoga incidenthanteringsrutinen. Bifoga också en sammanställning av utfallet av användningen av denna.