CHECKLIST BEOORDELEN ASSURANCE-VERKLARINGISAE 3402 type II, SOC 2 type II of alternatieve verklaring

Hulpmiddel bij beoordeling geschiktheid assurance-verklaringen

Afbeelding met tekst, wolk, silhouet

Automatisch gegenereerde beschrijving

Opgesteld door Insurance ISAC | Verbond van Verzekeraars | Versie: maart 2023

|  |  |
| --- | --- |
| Informatie over partner/service provider | |
| **Outsourcing partner/service provider** |  |
| **Applicatie/service/activiteit/dienst** |  |
| **Sub-service organisatie(s)** |  |
| **Afgegeven BIV/CIA classificatie** |  |
| **Soort en type verklaring** | *ISAE3402 type II / SOC 2 type II ?* |
| **Naam rapportage** |  |
| **Beoordelaar** |  |
| **Datum beoordeling** |  |
| **Goedkeurder/verantwoordelijke** |  |
| **Datum goedkeuring** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Algemeen | | | |
| Periode waarover (ISAE / SOC) assurance verschaft | *202x* | | |
| Is de periode dekkend voor de dienstverlening?  Zo nee, is er een bridgeletter? | *Ja/Nee, bij Nee aangeven of bridgeletter aanwezig is en of die dekkend is.* | | |
| Zijn de testen door een externe accountant uitgevoerd (naam toevoegen)? | *Een ISAE3402-assurancerapport kan alleen door een ingeschreven Register EDP-auditor (RE) of Register Accountant (RA) worden verstrekt.* | | |
| Volgens welke beroepsregels/vakorganisatie is het rapport afgegeven? | *NOREA, NBA, IIA, AICPA* | | |
| Is de reputatie van auditor van voldoende niveau? | *Ja/Nee* | | |
| Juiste soort assurance-rapportage?  - Voor Kritieke Diensten: ISAE3402 type II, SOC2  - Voor Jaarrekening: ISAE3402 of SOC1  - Voor ICT Dienstverlening: SOC2 | *Ja/Nee* | | |
| Een ‘auditor’s report’ is bij de door de serviceorganisatie opgestelde assurance-rapportage opgenomen? | *Ja/Nee* | | |
| Is een bewering (statement) van het management van de serviceorganisatie opgenomen (incl. management reactie)? | *Ja/Nee* | | |
|  |  | | |
|  | Afdoende = Geen issue | Niet afdoende = issue | *Toelichting/*  *interne maatregelen/*  *aandachtspunten* |
| Scope | | | |
| Geeft de assurance-verklaring over de volledige scope van de belangrijkste afgenomen diensten (incl. evt. maatwerk)? |  |  |  |
| Hoe wordt zekerheid gekregen over het deel wat niet door de assurance-verklaring wordt afgedekt? |  |  |  |
| Zijn er risico’s die niet worden afgedekt? |  |  |  |
| Zijn deze risico’s geaccepteerd door het management (<1 jaar)? |  |  |  |
| Bevat het rapport een hoofdstuk met relevante wijzigingen (bijv. processen toegevoegd, verwijderd)? Heeft dit consequenties voor de scope van het rapport? |  |  |  |
| Zijn de testwerkzaamheden en testresultaten beschreven in het assurance-rapport (o.a. steekproeven, beoordeling eigen waarnemingen, interviews)? |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Afdoende = Geen issue | Niet afdoende = issue | *Toelichting/*  *interne maatregelen/*  *aandachtspunten* |  |
| End User Complementary Controls (EUC) | | | |
| Zijn in de assurance-rapportage End User Complementary Controls (EUC) opgenomen? |  |  |  |  |
| Wordt er door de instelling invulling gegeven aan de gevraagde EUC’s? Zijn de maatregelen aantoonbaar effectief? |  |  |  |  |
| Zijn afspraken over de EUC’s terug te vinden in de SLA / DAP? Welke acties horen daarbij? Worden deze in structurele overleggen besproken? |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Carve-in/Carve-out (onderaannemers) | | | |
| Carve-in methode (opname/inclusive):  Bevat de verklaring ook sub-serviceorganisaties?  Zo ja, beantwoord dan de onderstaande drie vragen:   1. Is een beschrijving opgenomen van de services die door de sub-serviceorganisaties worden verleend? 2. Is opgenomen dat de sub-serviceorganisaties voldoen aan dezelfde eisen als de serviceorganisatie m.b.t. informatiebeveiliging en privacy? 3. Is aangegeven, waar van toepassing, dat specifieke beheersingsmaatregelen bij de sub-serviceorganisatie liggen? |  |  |  |
| Carve-out methode (uitsluiting):  Zijn er afzonderlijke rapportages van alle relevante dienstverleners (sub-serviceorganisaties)?  Zo ja, beantwoord dan de onderstaande drie vragen:   1. Zijn de door de sub-serviceorganisatie verleende diensten relevant voor de controle van financiële overzichten van instelling? 2. Heeft (interne)accountant dezelfde assurance-standaard toegepast op de sub-serviceorganisatie? 3. Zijn hieruit bevindingen naar voren gekomen? |  |  |  |