Waarom een ISAE 3402

Veel (gebruikers)organisaties besteden delen van hun activiteiten uit aan serviceorganisaties. Het betreft steeds vaker activiteiten die bij verstoring een grote impact kunnen hebben op de gebruikersorganisatie. Daarom is het continue goed functioneren van de serviceorganisatie van essentieel belang voor de gebruikersorganisatie. Afspraken over de dienstverlening worden vaak vastgelegd in een Service Level Agreement (SLA). De SLA biedt over het algemeen echter niet voldoende zekerheid over de kwaliteit van de dienstverlening van de serviceorganisatie.

Dit is de reden waarom de gebruikersorganisatie periodiek gerapporteerd wil worden over de kwaliteit van de uitbestede activiteiten door een onafhankelijke auditor. De rapportage over uitbestede activiteiten heet een ISAE 3402-verklaring.
Met de ISAE 3402-verklaring toont de serviceorganisatie aan in hoeverre zij voldoet aan de kwaliteitseisen van de gebruikersorganisatie. Deze informatie is van belang voor de gebruikersorganisatie om vast te stellen in hoeverre zij in control zijn over de uitbestede activiteiten.

Officiële status van ISAE 3402

Op 18 december 2009 heeft de IAASB de TPA-standaard gepubliceerd: de ISAE 3402 (International Standard for Assurance Engagements). De ISAE 3402 heeft in 2013 de SAS70 standaard vervangen. De ISAE 3402-verklaring is een internationale standaard die door nationale beroepsorganisaties, zoals de Nederlandse Beroepsorganisatie voor Accountants (NBA) en Nederlandse Organisatie Register EDP-auditors (NOREA), is opgenomen in hun body of standards. Hierdoor mogen Register accountants (RA) en Register EDP-auditors (RE) de verklaring afgeven.

Meer dan alleen financiële processen

De ISAE 3402 kent een uitgebreidere scope dan de SAS70 waardoor deze voor een bredere soort activiteiten is toe te passen. De scope beperkt zich niet tot de beheersmaatregelen voor de financiële processen. Ook zaken als betrouwbaarheid van het primaire proces, informatiebeveiliging en continuïteit kunnen worden opgenomen in een ISAE 3402-rapport. De nadruk ligt met name op de beheersmaatregelen die de uitbestedende organisatie verwacht aan te treffen.

De ISAE 3402 type 1 versus de ISAE 3402 type 2

De ISAE 3402 kent twee typen rapportages, het type I-rapport betreft een momentopname. Hierin wordt beschreven hoe een het proces en de beheersingsmaatregelen zoals deze op een bepaald moment zijn geïmplementeerd. De auditor toetst de haalbaarheid van de beschreven beheersingsmaatregelen om de gestelde beheersingsdoelstelling te bereiken en stelt de implementatie ervan vast. Een type I-rapport moet worden gezien als informatief rapport. Het ontbreken van zekerheid over de werking betekent dat het rapport geen direct bewijs levert voor de oordeelsvorming over de uitkomsten van het proces.

Het type II-rapport betreft een periode, meestal zes maanden tot een jaar. Het rapport beschrijft het proces en de beheersingsmaatregelen zoals deze gedurende de gedefinieerde periode hebben gewerkt. De auditor toetst de haalbaarheid van de beschreven beheersingsmaatregelen voor het bereiken van de beheersingsdoelstelling en stelt vast dat de implementatie ervan gedurende de rapportageperiode in overeenstemming is met de beschrijving. Daarnaast wordt de effectiviteit (werking) van de beheersingsmaatregelen gedurende de rapportageperiode gecontroleerd.

Welk type ISAE 3402 is voor onze organisatie van toepassing?

Welk type moet worden uitgevoerd wordt vaak bepaald door de uitbestedende organisatie. Zij stellen veelal in een overeenkomst vast welke type rapport zij willen ontvangen. Als de serviceorganisatie zelf de keuze heeft adviseren wij om bij een eerste ISAE 3402-traject te beginnen met een type I. Op basis daarvan kan worden vastgesteld welke beheersmaatregelen nog moeten worden ingericht of moeten worden verbeterd. Nadat de verbetering is gebruikersorganisatie doorgevoerd kan na minimaal 6 maanden een type II worden uitgevoerd. 12secure-u adviseert uw bedrijf graag over welk type het beste geschikt is voor uw organisatie.

Organisaties die onderstaande diensten leveren komen in aanmerking voor een ISAE 3402:

- Uitvoeringsinstanties voor hypotheken en pensioenen
- Payroll organisaties
- App leveranciers
- Webbased software leveranciers
- Managed BI leveranciers
- Callcenters
- Vastgoedbeheer
- Hosting leverancier
- Cloud leveranciers
- SaaS leveranciers
- Datacenters
- Managed service leveranciers
- Internet providers
- Uitvoerings Instanties voor medische claims

Stappenplan uitvoering ISAE 3402

1. Scoping
   In deze fase zullen wij samen met u inventariseren welke activiteiten onderdeel uitmaken van de scope van het ISAE 3402-rapport. De beschreven activiteit wordt vervolgens vastgelegd in een scoping document dat kan worden gebruikt voor afstemming met de uitbestedende organisatie(s).
2. Risicoanalyse
   In deze fase zullen wij samen met u een risicoanalyse uitvoeren, waarin de mate van gevoeligheid voor externe en interne risico's in kaart wordt gebracht. Op basis van de risicoanalyse wordt per activiteit duidelijk met welke risico's rekening moet worden gehouden bij het formuleren van de beheers doelstellingen en -maatregelen.
3. Beheers doelstellingen en -maatregelen
   Op basis van de scoping en de risicoanalyse wordt vastgesteld wat de beheers doelstellingen en –maatregelen moeten zijn. Vastgesteld moet worden per risico en per activiteit, welke maatregelen genomen dienen te worden om het risico te mitigeren. De beheersmaatregelen dienen ingebed te zijn in de organisatie middels o.a. beleid, processen en werkinstructies. De auditor zal op basis van de beheers doelstellingen en –maatregelen het werkplan voor de audit opstellen.
4. Pré-audit en Gap remediation
   12secure-u zal op basis van de beheersmaatregelen en de wijze waarop deze zijn geborgd in de organisatie een pré-audit uitvoeren. De serviceorganisatie dient vervolgens de eventueel gebleken leemtes en tekortkomingen op te pakken zodat de daadwerkelijke audit kan

worden uitgevoerd. Indien tijdens de pré-audit blijkt dat er geen leemtes of tekortkomingen zijn kan direct gestart worden met de audit.

5. Audit volgens de ISAE 3402-standaard
   12secure-u voert de audit volgens de ISAE 3402-standaard uit. De activiteiten die worden onderzocht zijn gedefinieerd in het scopings document. De criteria die worden onderzocht bestaan uit de vastgestelde beheersmaatregelen van stap 3.
6. Afstemmen concept rapport en opleveren definitief rapport
   12secure-u stelt eerst een concept rapport op, deze wordt met u inhoudelijk doorgesproken. Vervolgens wordt aan u een definitief rapport opgeleverd.