

WHITEPAPER · ASSURANCE

ISAE 3402: zekerheid over uitbestede diensten

Hoe begin je, hoe lang duurt het, wat kost het en waar let je op?

Voor serviceorganisaties zoals SaaS-leveranciers, hostingpartijen, salarisverwerkers en administratiekantoren die hun klanten zekerheid willen bieden.

Heldere audits. Deskundige mensen. Normaal tarief.

Editie oktober 2026

IN HET KORT

Laat zien dat je klanten op je kunnen bouwen

Steeds meer organisaties besteden processen uit. Ze blijven wel zelf verantwoordelijk voor de beheersing ervan. Een ISAE 3402-rapport laat met onafhankelijke zekerheid zien dat jouw dienstverlening onder controle is.

Met één rapport beantwoord je de vragen van al je klanten en hun accountants tegelijk. Dat scheelt audits, vragenlijsten en discussies. En het traject zelf maakt je organisatie sterker: processen worden scherper beschreven en risico's beter beheerst.

In deze whitepaper lees je wat ISAE 3402 is, wie het nodig heeft, hoe het traject verloopt, hoe lang het duurt en wat het kost.

Type I

Momentopname: is de opzet goed en zijn de maatregelen ingevoerd?
Doorlooptijd 1 tot 3 maanden.

Type II

Over een periode van meestal 6 tot 12 maanden: werken de maatregelen ook echt?

± 35

Beheersmaatregelen is een gangbaar aantal voor een gemiddelde serviceorganisatie.

Wat je in deze whitepaper vindt

Onderdeel	Wat je eraan hebt
1. Wat is ISAE 3402?	De standaard en de voordelen in een notendop
2. Wie heeft het nodig?	Typische serviceorganisaties en wettelijke achtergrond
3. De rapportage	Type I of II, de opbouw, en ISAE 3402 naast ISAE 3000 en SOC 2
4. Het traject	Negen stappen, de doorlooptijd en hoe je versnelt
5. De kosten	Indicatieve prijzen naar omvang van je organisatie

1 · WAT IS ISAE 3402?

Zekerheid die verder gaat dan een SLA

Veel organisaties besteden activiteiten uit aan een serviceorganisatie. Vaak gaat het om processen die bij een verstoring grote impact hebben, zoals salarisverwerking, hosting of financiële administratie. De afspraken staan in een Service Level Agreement, maar een SLA zegt niets over hoe goed de leverancier zijn processen écht beheerst.



Daarom willen gebruikersorganisaties, en hun accountants, periodiek een oordeel van een onafhankelijke auditor. Dat oordeel is het **ISAE 3402-rapport**: een internationale standaard (in Nederland: Standaard 3402) voor rapportages over de interne beheersing bij serviceorganisaties, met de nadruk op processen die de jaarrekening van de klant raken.

Wat levert het je op?

Wereldwijd erkend

Klanten, accountants en toezichthouders herkennen en accepteren het rapport, in Nederland en daarbuiten.

Minder audits

Accountants van je klanten kunnen op het rapport steunen. Je hoeft niet elke klant apart te woord te staan.

Sterkere organisatie

Processen worden scherper beschreven en risico's beter beheerst. Daardoor stuur je je bedrijf beter aan.

2 · WIE HEEFT HET NODIG?

Als jouw dienst de jaarrekening van je klant raakt

Organisaties blijven eindverantwoordelijk voor processen die ze uitbesteden. Ze willen dus weten hoe hun leverancier omgaat met risicomanagement, informatiebeveiliging en fraudebeheersing. Denk aan vragen als: *hoe wordt mijn data opgeslagen, hoe gaan jullie om met wijzigingen, en voldoen jullie aan de AVG?*

Typische serviceorganisaties

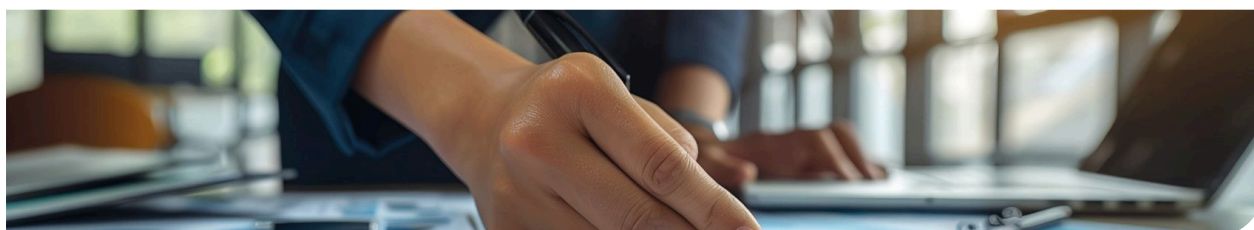
- SaaS- en softwareleveranciers
- Hosting- en cloudleveranciers
- Datacenters
- Managed service providers
- Payroll- en salarisverwerkers
- Pensioen- en hypotheekuitvoerders
- Administratie- en vastgoedbeheerders
- Leveranciers van BI-oplossingen
- Callcenters en klantcontactcentra
- Uitvoerders van (medische) declaraties

Waarom de vraag blijft groeien

Applicaties draaien steeds vaker als SaaS in de cloud, bij partijen als AWS, Microsoft of Google. Gebruikers hebben daardoor weinig zicht op de beveiliging. Tegelijk vragen accountants bij uitbestede, jaarrekeningrelevante processen om zekerheid. Een ISAE 3402-rapport is dan de gangbare oplossing.

Wet- en regelgeving

- **Financiële sector:** banken, verzekeraars en pensioenfondsen moeten volgens de Wft en de Pensioenwet aantonen dat ze uitbestede processen beheersen. Sinds januari 2025 stelt de Europese DORA-verordening daarnaast strenge eisen aan het beheer van ICT-dienstverleners.
- **Accountantscontrole:** heeft de serviceorganisatie een ISAE 3402-rapport, dan hoeft de accountant van de klant de uitbestede processen meestal niet zelf opnieuw te controleren.



3 · DE RAPPORTAGE

Type I of type II?

	Type I	Type II
Wat	Momentopname op een vaste datum	Periode, meestal 6 tot 12 maanden
De auditor toetst	Opzet en bestaan: zijn de maatregelen geschikt en ingevoerd?	Opzet, bestaan én werking gedurende de hele periode
Waarde voor de klant	Informatief; nog geen bewijs dat het werkt	Volwaardig bewijs waarop een accountant kan steunen
Wanneer	Eerste traject, om de basis neer te zetten	Zodra de maatregelen stabiel werken; daarna jaarlijks

Vaak bepaalt je klant in het contract welk type hij wil ontvangen. Heb je zelf de keuze? Begin dan met type I. Je ziet direct welke maatregelen nog verbeterd moeten worden. Zijn die op orde, dan volgt een type II over een periode van minimaal zes maanden.

Hoe ziet het rapport eruit?

De vorm is grotendeels vrij, maar een aantal onderdelen is verplicht: het oordeel van de auditor, een verklaring van het management, een beschrijving van je organisatie en risicomanagement, en een **control matrix** met beheersdoelstellingen en -maatregelen. Auditvision heeft sjablonen klaarliggen, zodat je snel kunt starten.

ISAE 3402, ISAE 3000 of SOC 2?

Standaard	Wanneer kies je hiervoor?
ISAE 3402	Je verwerkt financieel relevante informatie voor klanten, zoals salarissen of administratie.
ISAE 3000	Je wilt zekerheid geven over andere onderwerpen; je bepaalt zelf het normenkader en de reikwijdte.
SOC 2	Je klanten vragen een internationaal herkenbaar rapport over security, beschikbaarheid of privacy, met vaste criteria.

Ze overlappen deels. Het is mogelijk om ISAE 3402 en SOC 2 in één audit te combineren. We bespreken graag wat voor jouw klanten het meest logisch is.

4 · HET TRAJECT

Van kick-off tot rapport in negen stappen

Geen dagenlange sessies bij je op kantoor. Je verzamelt het bewijs wanneer het jou uitkomt in een omgeving die wij inrichten. Daarna beoordelen en verfijnen we het samen.



4 · HET TRAJECT

Hoe lang duurt het?

Elke organisatie is anders en ISAE 3402 is een flexibel kader zonder vaste maatregelen. Toch kunnen we op basis van ervaring een richting geven: een **type I** kost doorgaans één tot drie maanden, een **type II** zes tot twaalf maanden. De doorlooptijd hangt af van:

- de volwassenheid van je processen en beleid
- de omvang van je organisatie
- het aantal betrokken medewerkers
- het aantal beheersmaatregelen
- de betrokkenheid van het management

Voorbeeldplanning type I (in weken)



Werk terug vanaf een harde deadline en geef elke stap een eigen mijlpaal. Zo blijft het traject op schema.

Vijf manieren om te versnellen

- 1 Doe het niet alleen**
 Zeker de eerste keer helpt ervaring aan je zijde. De standaard biedt weinig houvast bij het kiezen van maatregelen.
- 2 Wees eerlijk over tekortkomingen**
 Wie zwakke plekken in de gap-analyse verbloemt, struikelt later tijdens de audit.
- 3 Zoek vroeg een auditor**
 De auditor helpt je de beste route te kiezen. Dat scheelt dubbel werk.
- 4 Maak een planning**
 Met een deadline weet iedereen wat er wanneer moet gebeuren.
- 5 Zorg voor steun van het management**
 HR, IT, legal en finance doen mee. Zonder steun van bovenaf verliest het project vaart.

4 · HET TRAJECT

Hoe kies je de juiste auditor?

Een ISAE 3402-traject doe je samen. Let daarom niet alleen op de prijs, maar vooral op de match.

1. Zoek flexibiliteit

Er is niet één juiste manier. Kies een auditor die jouw situatie vertaalt naar een passend normenkader, met kant-en-klare sjablonen waar dat kan.

2. Maak heldere afspraken

Stem de planning af en check of de auditor scope, risicoanalyse en bewijslast goed voor ogen heeft.

3. Let op de samenwerking

Een open, respectvolle samenwerking voorspelt het succes beter dan het contract.

4. Doe het samen

De auditor is niet de baas. Stel de agenda mee op en daag de auditor uit.

5. Betrek je team

Laat de medewerkers die meedoen vooraf kennismaken met de auditor.

6. Kies het team, niet het merk

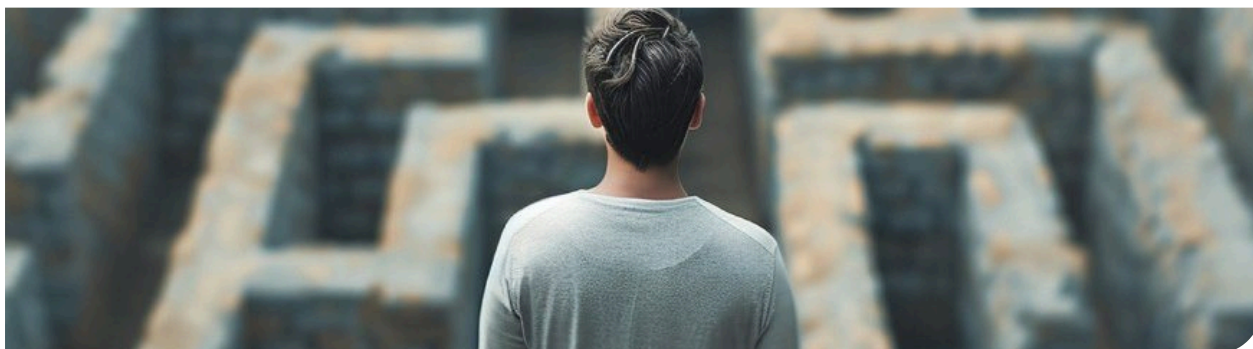
Een bekende naam zegt weinig. Het gaat om de mensen die jouw audit doen.

7. Praat met de uitvoerders

Spreek vooraf met de auditors en de teamleider, niet alleen met de verkoper.

8. Vraag referenties

Liefst van organisaties van vergelijkbare omvang, in dezelfde branche.



5 · DE KOSTEN

Wat kost een ISAE 3402?

Die vraag krijgen we vaak, zeker omdat er bedragen rondgaan die niet realistisch zijn. Een exact antwoord hangt af van je situatie, maar we geven je graag een eerlijke indicatie.

Uitgangspunt is een organisatie met circa 35 beheersmaatregelen en ons uurtarief van € 150. De bedragen zijn inclusief alle stappen, dus niet alleen de audit zelf. Bij type I gaat de meeste tijd naar begeleiding, bij type II naar het beoordelen van bewijs. Na de eerste type II daalt de inspanning in de jaren erna.

Aantal medewerkers	Type I	Type II	Volgende jaren
Minder dan 25	€ 8.000	€ 8.000	€ 7.000
25 tot 100	€ 12.000	€ 12.000	€ 10.000
100 tot 250	€ 15.000	€ 15.000	€ 12.000
250 tot 1.000	€ 20.000	€ 20.000	€ 15.000
Meer dan 1.000	op aanvraag	op aanvraag	op aanvraag

Indicatieve bedragen, exclusief btw. Je ontvangt altijd vooraf een offerte op basis van je eigen scope.

Onze werkwijze in drie woorden

Meedenken

Voor veel klanten is ISAE 3402 nieuw. We begeleiden je door elke stap.

Pragmatisch

De aanpak past bij de omvang en diensten van jouw organisatie.

Betaalbaar

Efficiënt werken met een vaste aanpak scheelt jou tijd en geld.



SAMEN AAN DE SLAG

Zo helpt AudITvision

AudITvision is een onafhankelijk IT-auditkantoor met een persoonlijke aanpak, vakmanschap en een eerlijke prijs. We maken complexe audits helder, begrijpelijk en werkbaar.

- **ISAE 3402 type I en type II:** van scoping tot definitief rapport.
- **ISAE 3000 en SOC 2:** als je klanten om een ander of breder rapport vragen.
- **Sjablonen en begeleiding:** voor de beschrijving van je organisatie, risicoanalyse en control matrix.

Wil je weten welk rapport bij jouw klanten past? Neem contact op voor een vrijblijvend gesprek.

AudITvision B.V.

Van der Houven van Oordtlaan 2
7316 AH Apeldoorn

088 – 202 87 00

info@auditvision.nl

www.auditvision.nl

Heldere audits. Deskundige mensen. Normaal tarief.

Deze whitepaper geeft algemene informatie. De genoemde bedragen zijn indicatief. © AudITvision B.V., oktober 2026.