# ISAE 3402
# Wat moet je er mee?

**Een assurance-rapport is geen vinkje. Het is een instrument, maar alleen als je weet hoe je het moet lezen. Veel financiële instellingen hebben het afgelopen jaar flink geïnvesteerd in DORA-implementatie. Beleid staat op papier, leveranciers zijn geregistreerd en we kijken naar hun IT-security door middel van het ISAE 3402-rapport.**

**Maar wat staat er eigenlijk in zo'n rapport? En wat zegt het en wat zegt het níet?**
Die vragen zijn urgenter dan ze klinken. Want de NBA, NOREA en IIA Nederland waarschuwen in hun gezamenlijke publicatie Vertrouwen in de kwetsbare keten (2026) voor een hardnekkig misverstand: bestuurders verwachten soms méér zekerheid van assurance-rapporten dan die rapporten kunnen bieden.

> *Assurance geeft slechts zekerheid over een afgebakend deel van de werkelijkheid en over een specifieke periode. Niet over de keten als geheel.*
>
> NBA, NOREA & IIA Nederland,
> Vertrouwen in de kwetsbare keten, 2026

**Wat is een ISAE 3402-rapport?**
ISAE 3402 is een internationale standaard voor assurance bij uitbestede diensten. Een externe accountant of IT-auditor onderzoekt of de beheersmaatregelen bij een serviceleverancier bestaan én werken. Het rapport is bedoeld voor klanten van die leverancier zodat zij kunnen steunen op de bevindingen.
Er zijn twee varianten. Een type I geeft een oordeel over de opzet op één moment. Een type II gaat verder: die beoordeelt ook de werking over een periode van minimaal zes maanden. Voor grip op uitbestede risico's is een type II dus aanzienlijk waardevoller.

**Wat een ISAE 3402-rapport je vertelt**
Een ISAE 3402-rapport geeft inzicht in hoe een leverancier kritieke processen beheerst die de financiële verantwoording raken. Denk aan toegangsbeheer, wijzigingsbeheer, back-up en herstel, incidentopvolging en functiescheiding. Processen die verband houden met de financiële verantwoordingen.

De waarde zit in drie dingen: het geeft een grondslag voor je leveranciersbeoordeling, het biedt aanvullende zekerheid over specifieke onderdelen, en het levert gespreksstof op met de leverancier, met interne audit en met het bestuur.

## ISAE 3402 in de PDCA-cyclus

**Plan**
- Stel eisen aan assurance per kritieke leverancier
- Leg scope-eisen vast in leveranciersbeleid
- Betrek interne audit vooraf bij de risicoanalyse

**Internal audit: adviseert over scope en criteria**

**DO**
- Bevorder het opstellen van ISAE 3402 rapportages door kritieke leveranciers
- Registreer ontvangen security rapportages in het informatieregister
- Controleer of het rapport type II is en actueel
- Sla het rapport op, klaar voor inhoudelijke review

**Internal audit: toetst of proces wordt gevolgd**

**Act**
- Ga in gesprek over mogelijke verbeteringen
- Beslis: aanvullende assurance of contract-aanpassing
- Rapporteer restrisico's aan bestuur en compliance
- Gebruik leerpunten voor volgende Plan-fase

**Internal audit: bewaakt opvolging van bevindingen**

**Check**
- Beoordeel scope: wat valt er buiten?
- Analyseer bevindingen en uitzonderingen
- Toets of gebruikerscontroles intern zijn belegd
- Koppel conclusies aan eigen risicoanalyse

**Internal audit: onafhankelijke toets op de review**

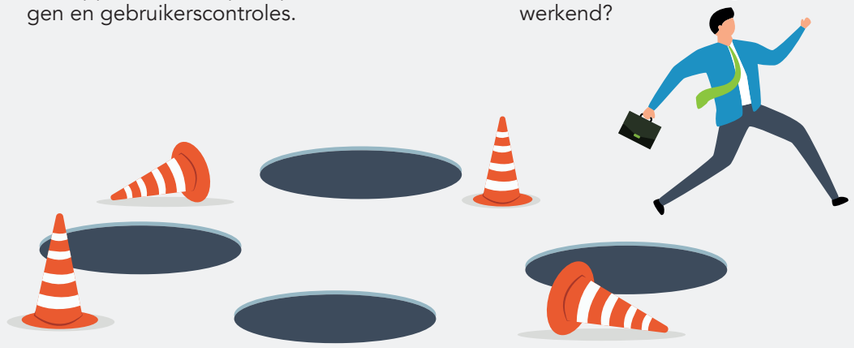
## De vier valkuilen bij assurance-rapporten

1. **Scope: wat valt er buiten?**
Welke diensten, systemen, locaties en onderaannemers zijn expliciet uitgesloten? Als iets niet is onderzocht, heb je geen zekerheid. En in hoeverre is het relevant voor het product of dienst dat je afneemt?

2. **Periode: hoe oud is de informatie?**
De rapportages kijken terug, maar hoe is het nu? Tussen het einde van de onderzochte periode en het moment van publicatie kunnen nieuwe risico's zijn ontstaan.

3. **Carve-outs: wat is weggelaten?**
Delen van de dienstverlening kunnen buiten het onderzoek zijn gebleven. Lees het rapport kritisch op scope, uitsluitingen en gebruikerscontroles.

4. **Gebruikerscontroles: uw eigen verantwoordelijkheid**
Veel rapporten benoemen maatregelen die u zelf moet uitvoeren. Zijn deze inderdaad intern belegd en aantoonbaar werkend?



**Wat een ISAE 3402-rapport je níet vertelt**
Hier gaat het in de praktijk vaak mis. Een ISAE 3402-rapport dekt altijd een afgebakende scope en periode. Wat buiten die scope valt, is niet beoordeeld en dat kan veel zijn. Onderaannemers van de leverancier vallen er vaak buiten. Crisismanagement, exitplannen en cyberveerkracht ook. Het rapport gaat over de afgelopen periode, maar de wereld is dynamisch.

**Geen DORA-vinkje**
De belangrijkste valkuil is dat een ISAE 3402-rapport wordt gezien als bewijs dat de leverancier "DORA-compliant" is. Dat is het niet.
ISAE 3402 is geen DORA-certificaat. Het is ook geen algemene verklaring dat een leverancier volledig in control is. De bruikbaarheid hangt volledig af van de scope, de periode, de onderzochte beheersdoelstellingen, de uitkomsten van de testwerkzaamheden en de relevantie voor uw eigen risicoanalyse.

**Een assurancerapport is geen eindpunt**
Een rapport ontvangen is niet hetzelfde als grip hebben. De NBA, NOREA en IIA zijn hier helder over: assurance is een hulpmiddel, geen garantie. Het vergroot vertrouwen waar dat kan maar het neemt onzekerheid niet weg en vervangt het eigen oordeel nooit.

De betere vraag is dus niet: "Hebben wij een ISAE 3402-rapport ontvangen?", maar: "Wat leert dit rapport ons over de werking van onze ketenbeheersing, en wat verbeteren we in de volgende cyclus?"

Juist daar ligt de meerwaarde van een goede interne auditfunctie: onafhankelijk toetsen, scherp doorvragen en helpen voorkomen dat aanvullende zekerheid wordt verward met volledige zekerheid.