

IT-ASSURE

Zekerheid over uw IT



NOREA

de beroepsorganisatie van IT-auditors

- 
- 3 Steeds meer behoefte aan onafhankelijk oordeel over IT
 - 5 Grotere zekerheid over kwaliteit van IT
 - 6 Outsourcing Assurance
 - 8 Project Assurance
 - 9 IT-organisatie Assurance
 - 9 Applicatie Assurance
 - 9 IT Due Diligence
 - 10 Privacy Assurance
 - 10 Web Assurance
 - 11 Revenue Assurance
 - 11 Licentie Assurance

NOREA

de beroepsorganisatie van IT-auditors

©2008 NOREA
tekst Joop K. de Vries
redactie Wilfried Olthof
productie LINE UP boek en media
design Jan Faber (LINE UP)
beeld asifthebes (www.sxc.hu)
ISBN 978 90 77487 65 5



Steeds meer behoefte aan onafhankelijk oordeel over IT

IT maakt de bedrijfsprocessen in uw organisatie steeds effectiever en efficiënter. Tegelijkertijd wordt u steeds afhankelijker van IT. Dat vergroot de behoefte aan betrouwbare systemen om inkomstenderving, reputatieschade

en schadeclaims te voorkomen. Zekerheid over de kwaliteit van IT is ongetwijfeld ook in uw organisatie van groot belang. Niet alleen omwille van de continuïteit en kwaliteit van uw vitale bedrijfsprocessen, maar ook vanwege de hoge eisen die tegenwoordig worden gesteld aan transparantie, IT-governance (goed ondernemingsbestuur) en compliance (voldoen aan wet- en regelgeving). Hoge eisen gelden ook voor (deels) uitbestede of ingehuurd diensten of voor dataverwerking en -opslag in shared service-centra. Zekerheid over al uw IT krijgt u door een onafhankelijke Register IT-auditor (RE) een IT-assuranceonderzoek uit te laten voeren.

IT-assurance kan zekerheid bieden over elk denkbaar IT-object. Bij een assuranceopdracht is doorgaans sprake van drie partijen: ten eerste een partij die zich verantwoordt, ten tweede de toetsende IT-auditor en ten derde een partij die gebruikmaakt van de uitkomsten van het onafhankelijke oordeel van de IT-auditor. De gebruiker wil objectieve informatie ontvangen over de mate waarin de dienstverlening in overeenstemming is met de afgesproken eisen. Met die informatie kan bijvoorbeeld het management of de raad van bestuur beoordelen of de outsourcing van het rekencentrum in India in control is, maar ook of een groot project volgens planning verloopt. Een toezichthoudende autoriteit die eist dat de Wet bescherming persoonsgegevens binnen uw bedrijf wordt nageleefd, zal deze informatie ook gebruiken. Het gaat kortom om het versterken van het vertrouwen in de zich verantwoordende partij.

Gedragscode beroepsorganisatie NOREA

De vereniging Nederlandse Orde van Register EDP-Auditors (NOREA) is de beroepsorganisatie van IT-auditors. De organisatie heeft zo'n 1400 leden en ruim 500 aspirant-leden. NOREA kent een Reglement Gedragscode, gebaseerd op de Code of Ethics van de International Federation of Accountants (IFAC), waarbij de NOREA ook is aangesloten. Assuranceopdrachten worden in dat verband ook uitgevoerd volgens het internationale IFAC-Raamwerk en de Richtlijnen voor Assuranceopdrachten. De IFAC/NOREA Richtlijn 3000 stelt eisen aan de kwaliteit en uitvoering van de opdracht, de inhoud van het assurancerapport en de wijze waarop het oordeel wordt geformuleerd.

De Register IT-auditor (RE): uw onafhankelijke en betrouwbare partner

Register IT-auditors zijn op grond van hun opleiding en ervaring de aange-
wezen deskundigen om IT-assurance-
opdrachten uit te voeren. IT-auditors
hebben de erkende masteropleiding tot
IT-auditor voltooid en kunnen tenmin-
ste drie jaar praktijkervaring aantonen.
Pas dan kunnen ze zich laten inschrij-
ven als Register EDP-auditor (RE). Met
inschrijving in het register verbinden
ze zich aan de gedrags- en beroeps-
regels en zijn ze onderworpen aan
tuchtrechtspraak. RE's hebben kennis
van informatietechnologie, bestuurlijke
informatievoorziening, organisatie-
kunde en methoden en technieken van
onderzoek, toetsing en risicoafweging.
Bovendien hebben zij ervaring met
kosten van IT en toepassingsgebieden.
Een RE geeft onpartijdige adviezen
en oordelen over kwaliteitsaspecten
van IT. Daarmee vult hij de register-
accountant aan die met name de cijfers
controleert. De toegevoegde waarde
van de RE wordt inmiddels onderkend
door toezichthouders als de Neder-
landsche Bank, de Autoriteit Financiële
Markten en het College bescherming
persoonsgegevens.

Redelijke of beperkte mate van zekerheid

Absolute zekerheid dat er nooit iets mis zal gaan met IT
in uw organisatie krijgt u nergens. Ook niet bij een RE.
Bij IT-assurance spreekt u vooraf met de RE de diepgang
van het onderzoek af; die diepgang is veelal bepalend voor
de mate van zekerheid die kan worden verleend. Daarbij
wordt onderscheid gemaakt tussen een redelijke mate van
zekerheid en een beperkte mate van zekerheid. Bij een
redelijke mate van zekerheid verklaart de IT-auditor dat het
onderzochte IT-object tijdens het onderzoek voldeed aan de
afgesproken normen. Letterlijk verklaart hij: "Op grond van
ons onderzoek zijn wij van oordeel dat op de onderzoeks-
datum de opzet en het bestaan van
de maatregelen en procedures ter
waarborging van de exclusiviteit,
integriteit, controleerbaarheid en
continuïteit van het onderzochte
informatiesysteem in alle van
materieel belang zijnde opzichten
hebben voldaan aan de normen."
Bij een beperkte mate van zeker-
heid verklaart de IT-auditor dat
hij geen belangrijke afwijkingen
van de gemaakte afspraken heeft
geconstateerd. De zekerheid is
beperkt omdat vooraf is afgespro-
ken dat niet alle aspecten van
het onderzoeksobject diepgaand
worden onderzocht. De defini-
ties over zekerheid zijn opgesteld
door de International Federation
of Accountants (IFAC) en worden
wereldwijd gehanteerd.

RE doet meer dan alleen IT-assurance

U kunt een RE voor meer inscha-
kelen dan alleen IT-assurance.
Een RE kan meedenken en advi-
seren over alle informatietech-
nologie in een organisatie. De RE
is een professional die op grond
van zijn opleidingen en praktijk-
ervaring beschikt over de juiste
deskundigheid met betrekking
tot softwarepakketten, projec-
ten, beheersing en beveiliging.
Naast het uitvoeren van een
assuranceopdracht, zoals beschre-
ven in deze brochure, kan een RE
ook gewoon adviseren over de
genoemde onderwerpen.



Grotere zekerheid over kwaliteit van IT

Een IT-assuranceonderzoek kunt u instellen om zekerheid te krijgen over goed ondernemingsbestuur (governance), uw IT-risico's (risk) en of u voldoet aan wet- en regelgeving (compliance). RE's kennen de risico's en de relevante regelgeving en kunnen u daarover adviseren. Een IT-assuranceonderzoek kan zich

richten op elk denkbaar IT-object, bijvoorbeeld het uitvoeren van IT-proces-
sen zoals technische of functionele beheerprocessen of het beschikbaar stel-
len van IT-faciliteiten zoals netwerkdiensten en uitwijkfaciliteiten.

RE's zijn onder meer actief op de gebieden IT-projectmanagement, outsour-
cing, informatiebeveiliging, privacycertificering, inkomsten uit licenties,
e-business en due diligence. Een RE kan worden gevraagd een oordeel te
geven over een bepaald object of aspect, maar kan ook een objectief oordeel
geven over een verantwoording die een bestuur heeft afgelegd. Hij stelt
dan vast of overeenkomstig de voorgestelde feiten is gerapporteerd. Een RE
maakt voorafgaand aan het assuranceonderzoek met u afspraken over reik-
wijdte, toetsingscriteria en auditstandaarden. Zodat u zekerheid krijgt over
uw specifieke situatie. Een IT-assuranceonderzoek kan zich, zoals gezegd,
richten op elk denkbaar IT-object. Het is daarmee ondoenlijk alle soorten on-
derzoek uitgebreid aan de orde te stellen. Enkele veelvoorkomende assurance-
onderzoeken zijn beknopt beschreven in deze uitgave. Voor meer informatie
kunt u natuurlijk terecht bij uw RE of zijn beroepsorganisatie, de NOREA.



Outsourcing Assurance

Inzicht in de kwaliteit van dienstverlening

Outsourcing Assurance biedt een uitbestedende organisatie zekerheid of een serviceorganisatie de aan haar uitbestede processen in haar greep heeft. Het management van de uitbestedende organisatie blijft immers eindverantwoordelijk voor deze processen. In toenemende mate wordt de behoefte aan zekerheid ook gevoed door wet- en regelgeving als de Code Tabaksblat, Sarbanes-Oxley, Wet Financieel Toezicht, Basel II en Solvency II. Outsourcing Assurance kunt u laten doen naar de beheersmaatregelen van elk proces of deelproces dat is uitbesteed, van IT en salarisverwerking tot en met processen op het gebied van administratie of logistiek.

TPM, SAS 70 of ISAE 3402

Outsourcing Assurance is maatwerk en wordt ingesteld voor een vooraf omschreven doelgroep. De serviceorganisatie en de uitbestedende organisatie zijn vrij te bepalen welke beheersdoelstellingen en processen ze opnemen in het onderzoek. Vroeger werd een assuranceopdracht ook wel een Third Party Mededeling (TPM) genoemd. Daarbij werd onderscheid gemaakt tussen een TPM zonder vormvoorschriften voor de wijze van rapporteren, en de sterk gestructureerde SAS 70-verklaring. SAS 70 is bedacht om te voorkomen dat serviceorganisaties voor verschillende klanten steeds dezelfde processen moeten (laten) beoordelen. SAS 70 staat voor Statement on Auditing Standards no. 70, een Amerikaanse auditingstandaard voor het documenteren van het stelsel van interne beheersmaatregelen met betrekking tot uitbestede processen, het auditen van deze maatregelen op hun toereikendheid en, naar keuze, de werking van deze maatregelen. De serviceorganisatie beschrijft in een SAS 70-rapport op hoofdlijnen de beheerorganisatie en geeft hierbij aan hoe zij specifieke beheersdoelstellingen bereikt. Een externe auditor voegt een rapport toe over de mate waarin die beheersdoel-

Ontevredenheid over ICT-dienstverlening naar recordhoogte

De enorme stijging van de ICT-budgetten en de vraag naar externe ICT'ers blijft groeien, zo blijkt uit het onderzoek. Ondanks deze groei is het met de ICT-dienstverlening verre van rooskleurig gesteld. Was er vorig jaar nog een zekere mate van tevredenheid waar te nemen, dit jaar is de ontevredenheid over de ICT-dienstverlening gestegen naar recordhoogte. Net als begin deze eeuw blijkt dat met het toenemen van de ICT-budgetten de kwaliteit van de ICT-dienstverlening afneemt.

Bron: *ICT-barometer.nl*, 31 juli 2007.

stellingen worden gerealiseerd. Het resultaat is dat de uitbestedende organisatie inzicht krijgt in de wijze waarop de uitbestede processen worden beheerst. Bovendien kan het rapport nuttig zijn voor de externe accountant van de uitbestedende organisatie bij de controle van de jaarrekening. Bij SAS 70 bestaan twee soorten onderzoek. Type I is een momentopname. Type II is een

uitspraak over een bepaalde periode van minimaal zes maanden. SAS 70 is gebaseerd op regelgeving in de Verenigde Staten en daardoor niet zomaar toepasbaar in andere landen. Daarom is een nieuwe internationale standaard ontwikkeld, de ISAE 3402. Deze is waarschijnlijk per eind 2008 beschikbaar.

Processen volgens afspraak

Een serviceorganisatie verzorgt de uitvoering van de verzekeringsadministratie voor een grote verzekeraar. De verzekeraar wil zeker weten dat de uitvoering van de processen verloopt volgens contractueel vastgelegde richtlijnen. De RE verstrekt deze zekerheid door het afgeven van een SAS 70-rapport aan de serviceorganisatie.

Effectieve software

De raad van bestuur van een grote Nederlandse instelling heeft recent een nieuw softwarepakket aangeschaft ter ondersteuning van de administratie. Het project is uitgevoerd en bijna afgerond. De gebruikers zijn echter ontevreden over de geboden oplossing. Een RE is gevraagd een onderzoek uit te voeren naar de mate waarin het gekozen pakket de administratie effectief ondersteunt.

Projectreviews vergroten slagingskans

Een fabriek wil zijn bestaande ERP-systeem volledig vervangen. Kosten: vele miljoenen. De impact op de bedrijfsprocessen is groot. Mislukken van het project kan leiden tot grote verliezen of wellicht zelfs faillissement. Door projectreviews brengt de RE de risico's in kaart en ondersteunt hij het management bij het vergroten van de kans dat het project met succes wordt afgerond.

Project Assurance kwaliteit (doorlopend) inzichtelijk gemaakt

Als u wilt weten of een project voldaan heeft aan de verwachtingen, kunt u na afronding Project Assurance laten uitvoeren. De impact van IT-projecten is de afgelopen jaren sterk toegenomen en daarmee ook de eisen rondom het welslagen van ICT-projecten. Door tijdens het project op cruciale punten een RE om assurance te vragen is een project doorlopend inzichtelijk en beter beheersbaar voor de stuurgroep. U kunt in overleg met een RE bepalen wat u beoordeeld wilt hebben, bijvoorbeeld projectplan, opzet van de projectorganisatie, coördinatie, voortgangsbewaking en rapportage, risicomangement, standaarden en procedures. Echter, deze projectreviews hebben eerder het karakter van een adviesopdracht dan een assurance-opdracht; met andere woorden, de beoordeling is bestemd voor de opdrachtgever.

Minder dan helft alle ICT-projecten volledig succesvol

Minder dan de helft van alle ICT-projecten is volledig succesvol. Van de overige 52 procent van de projecten faalt 4 procent volkomen, of 48 procent gedeeltelijk. De invoering van CRM-systemen leidt bijna niet tot succes: meer dan tweederde van deze projecten mislukt. Dat betekent meer dan 15.000 rampprojecten per jaar.

Bron: ICT-barometer.nl, 20 juni 2007.

IT-organisatie Assurance

structuur in processen en organisatie

IT-organisatie Assurance richt zich op de manier waarop IT en IT-processen in de organisatie zijn vormgegeven. Zijn er waar nodig functiescheidingen? Hoe zijn strategie, ontwerp, implementatie en beheer van IT-processen gepositioneerd? En hoe staat het met incident- en verandermanagement? De RE kan over dergelijke organisatieaspecten een oordeel uitspreken.

Applicatie Assurance

controle op invoer, verwerking en uitvoer

Bij Applicatie Assurance gaat het om controle op authenticatie, autorisatie, invoerverzorging zoals bestaanbaarheid, totalen, redelijkheid en volledigheid. En om controle op verwerking en uitvoerverzorging.

IT Due Diligence

samen goed op weg

Een Due Diligence brengt de risico's in kaart bij een overname, fusie of joint venture. Die risico's kunnen van velerlei aard zijn: financieel, fiscaal, juridisch en milieu-technisch. Bij een IT Due Diligence onderzoekt een RE welke risico's er kleven aan de over te nemen IT-omgeving. Waarbij onder andere wordt gekeken of IT-systemen de toekomstige bedrijfsvoering adequaat ondersteunen en of er investeringen nodig zijn.

Goed beltegoed

Een telecombedrijf heeft een applicatie voor het online opwaarderen van beltegoed ontwikkeld. Het bedrijf wil zowel aan zijn klanten als aan de accountant laten zien dat de applicatie betrouwbaar is. Een IT-auditor verschaft die zekerheid en beoordeelt daarbij onder meer de authenticatie van de klant en de beveiliging van de bankgegevens in het systeem.

Duidelijkheid kosten overgang ander ERP-systeem

Een van de grotere supermarktorganisaties in Europa wilde een fors aantal supermarkten verkopen. De overnemende partij werkte met een ander ERP-systeem dan de verkoper. Due Diligence gaf duidelijkheid over de waarde van het bestaande ERP-systeem van de verkoper dat uitgefaseerd zou worden, en over de kosten van het nieuw te implementeren systeem.

Wachtwoorden eenvoudig te ontfutselen

Wachtwoorden ontfutselen is eenvoudig geworden. Iedereen die een publieke dienst aanbiedt moet zich vandaag afvragen of gebruikersnaam en wachtwoord nog een voldoende basis van vertrouwen vormen. Voor steeds meer diensten worden maatregelen ingevoerd, zoals het gebruik van SSL, waarbij een digitaal certificaat de dienst identificeert aan de gebruiker. Nederlandse banken wapenen zich met two factor authentication, maar moeten blijven nadenken over volgende stappen en aanvullende maatregelen nemen.

Bron: GOVCERT.NL, het Computer Emergency Response Team van en voor de Nederlandse overheid, Trendrapport 2007.

Privacy Assurance zorgvuldig omgaan met persoonsgegevens

Privacy Assurance verschaft zekerheid over het voldoen aan privacyregels bij de verwerking van persoonsgegevens. Aan een privacy-audit is het keurmerk Privacy-Audit-Proof verbonden. Dit keurmerk is ontwikkeld door het Koninklijk NIVRA en de NOREA in overleg met het College bescherming persoonsgegevens (CBP). In Nederland stelt de Wet bescherming persoonsgegevens eisen aan de wijze waarop organisaties (zowel publiek als privaat) persoonsgegevens mogen verwerken.

Web Assurance betrouwbare e-commerce-applicaties

De handel via internet is de afgelopen jaren sterk toegenomen en daarmee zijn organisaties meer en meer afhankelijk geworden van de betrouwbaarheid van hun e-commerce-applicaties. De RE kan u helpen bij het verschaffen van zekerheid over de e-commerce-applicaties die u gebruikt.

Revenue Assurance

voorkom inkomstenderving

Revenue Assurance biedt een organisatie zekerheid dat klanten een correcte rekening krijgen en dat de organisatie geen inkomsten misloopt voor verleende diensten. Bij de verkoop van online-informatie zijn tal van partijen betrokken: eigenaren, aanbieders, distributeurs en afnemers. Deze partijen vertrouwen in veel gevallen op self-reporting als primair mechanisme voor het registreren van verkopen. Mede als gevolg hiervan zijn gegevens over de verkoop van online-informatie niet altijd betrouwbaar.

Licentie Assurance

precies genoeg betalen voor legaal gebruik

Licentiebeheer van software is altijd de verantwoordelijkheid van de gebruiker. Een veelvoud aan veelvormige contracten in combinatie met steeds mobieler en veeleisender wordende eindgebruikers doet het overzicht nogal eens verdwijnen. Licentie Assurance geeft u zekerheid over de juiste aantallen en soorten licenties. En over het legaal gebruik van software. Ook het certificeren van softwarepakketten kan worden opgevat als een assuranceopdracht.

Illegale software:
€36.000 boete

Bijna eenderde van de gebruikte pc-software in Nederland is illegaal, blijkt uit onderzoek van de Business Software Alliance, de speurhond naar illegaal gebruik van software. Bedrijven die door de BSA worden aangeklaagd, moeten een schadevergoeding betalen van gemiddeld €36.000.
Bron: BSA.nl, 15 maart 2007.

Licentiebeheer blijft enorme worsteling

Bedrijven die illegaal software gebruiken zijn doorgaans niet in de regel 'als de dood' voor een bezoek van de BSA, die ernstige reputatieschade kan veroorzaken, maar in de praktijk hebben deze bedrijven grote moeite om zich volledig aan de grote variatie van licentieregels te houden. De Business Software Alliance (BSA) bestaat uit een aantal softwareleveranciers die gezamenlijk optrekt tegen illegaal softwaregebruik.
Bron: Automatisering Gids, nr. 37 – 2007.



Meer informatie

NOREA, de beroepsorganisatie van IT-auditors

Postbus 7984

1008 AD Amsterdam

Tel: (020) 301 03 80

Fax: (020) 301 03 02

E-mail: NOREA@NOREA.nl

Internet: www.NOREA.nl