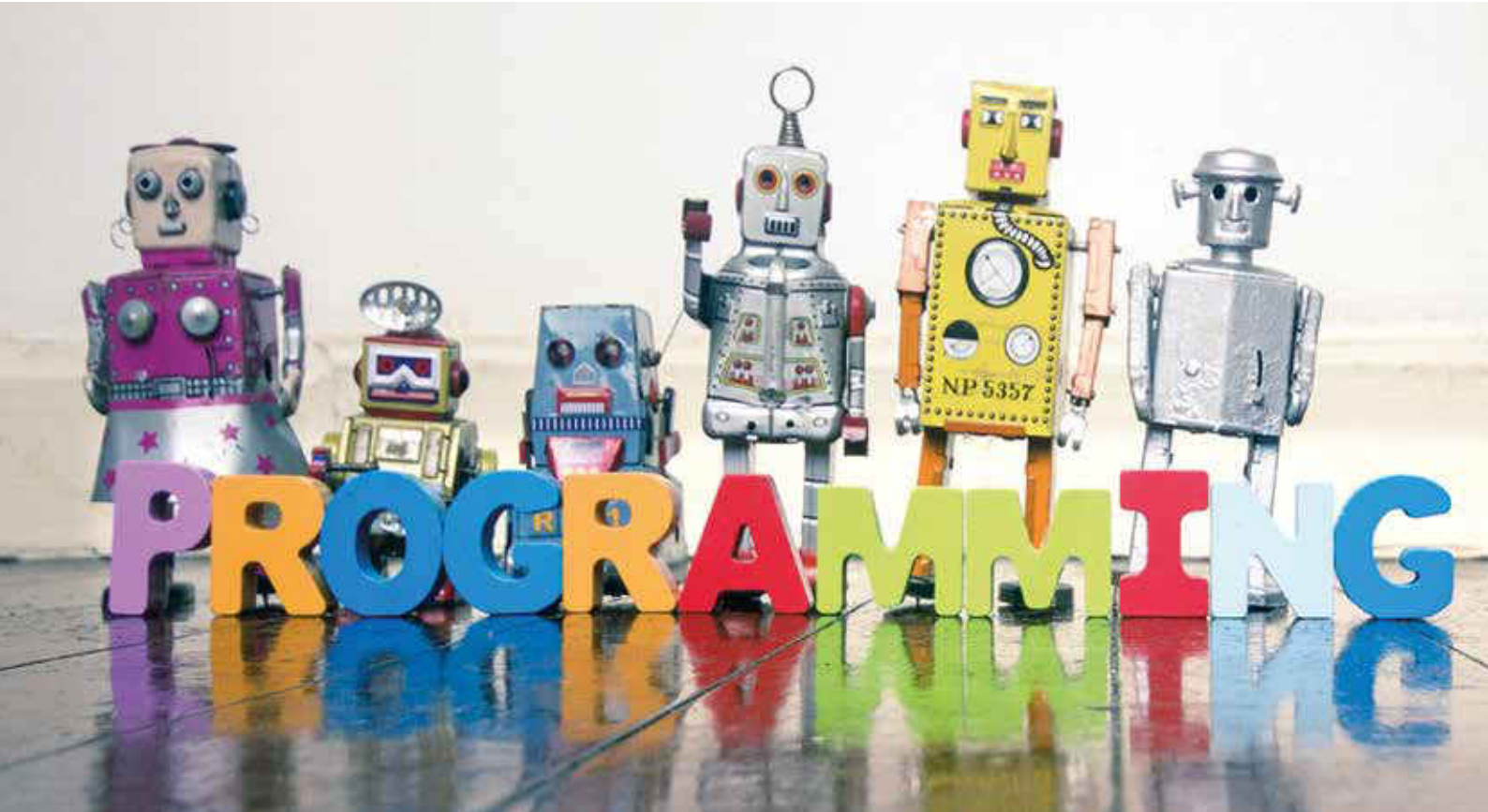
Thema Complexe technologie
Tekst Steven Boekhoudt MSc
Beeld Adobe Stock

De opkomende technologie robotics process automation (RPA) doet in steeds meer organisaties haar intrede. Dit artikel gaat in op de nieuwe uitdagingen en RPA-specifieke risico's en relateert deze aan de COBIT IT-controleprocessen die als handvatten dienen voor internal auditors om de interne beheersing rondom RPA te beoordelen.

Wat vinden **robots** van COBIT?



RPA is een technologie die hoogvolume gestandaardiseerde, repetitieve, veelal voor de mens onaantrekkelijke taken vervangt door softwarerobots. De voordelen hiervan zijn dat deze robots zonder onderbreking kunnen doorwerken en taken consistent uitvoeren op basis van vooraf geprogrammeerde regels. De RPA-technologie is zo ontworpen dat het geen hoge investeringskosten kent en dat deze moeiteloos integreert met applicaties in het huidige IT-landschap, waardoor de robots snel werken en winst kunnen opleveren.

Zelf software bouwen

De belangrijkste en meest vernieuwende eigenschap van RPA is dat het de business zelf in staat stelt om software (robots) te bouwen. Waar voorheen het ontwikkelen van software het exclusieve domein van de IT-functie was, is het voor gebruikers met een minder technische achtergrond aanzienlijk toegankelijker geworden om softwarecode te schrijven. Onder andere zogenaamde 'drag & drop'-functionaliteiten, het opnemen ('screenrecording') van processen en een gebruiksvriendelijke 'user interface' (UI) maken het bouwen van een robot een stuk eenvoudiger. In de praktijk is dan ook zichtbaar dat de meeste RPA-initiatieven vanuit de business beginnen.

Deze verschuiving in kunde resulteert in nieuwe en specifieke RPA-risico's voor organisaties die (veelal meerdere) robots willen implementeren. Werknemers zonder IT-achtergrond zijn nu in staat robots te programmeren. Daar komt bovenop dat uit verschillende, door de big four uitgevoerde, enquêtes (gehouden bij meer dan 150 organisaties) blijkt dat een van de belangrijkste pijnpunten bij de implementatie van RPA is dat de IT- afdeling en de business onvoldoende geïntegreerd zijn. Dit leidt tot grote risico's met potentieel verstrekkende gevolgen als er geen adequate interne beheersing rondom RPA wordt ingericht.

COBIT: handvatten voor samenwerking

Het algemeen aanvaarde IT-governanceraamwerk COBIT is erop gericht om 'good-practice'-handvatten te bieden om de samenwerking tussen IT en business effectief in te richten aan de hand van 34 IT-controleprocessen.[1] De vraag is alleen of het implementeren van COBIT nog steeds een voldoende mate van interne beheersing geeft in de context van RPA. Om dit vast te stellen voerde PwC een onderzoek uit (op 08/2018), gericht op het identificeren van RPA-specifieke risico's. Deze risico's zijn vervolgens gerelateerd aan de IT-controleprocessen van COBIT. Hierna worden eerst de risico's kort behandeld en daarna worden deze gerelateerd aan de IT-controleprocessen van COBIT.

R1 Change management

Robots maken gebruik van zogenaamde 'selectors' waarin informatie is opgeslagen over een bepaald zichtbaar onderdeel op de UI. De werking is vergelijkbaar met een HTML-code van een website waarin de opbouw en de tekst staat beschreven. Aan de hand van deze selectors kan de robot dus een deel van het scherm identificeren en er een actie op uitvoeren. Dit kan op verschillende applicaties, systemen, internetwebsites, Microsoft Office en alles wat een gebruiker ziet op de UI. Deel van deze identificatie kan de kleur van een button zijn of de geschreven tekst die erop staat. Op het moment dat een of meerdere identificatiekenmerken wijzigen, komt de selector niet meer overeen met de UI en kan de robot de geprogrammeerde acties niet meer uitvoeren.

De belangrijkste en meest vernieuwende eigenschap van RPA is dat het de business zelf in staat stelt om software (robots) te bouwen

Een goed werkend change-managementproces is dan ook essentieel, maar tegelijkertijd ook een ware uitdaging bij het opschalen naar meer robots.

R2 Afhankelijkheid van werknemers

Een robot bouwen is bij uitstek een combinatie van IT en de business. Waarbij de business vooral de kennis over de te robotiseren processen zal aanleveren en IT zich meer richt op vraagstukken als toegang en het onderhoud van de robots. Robots worden veelal gebruikt om manuele processen te vervangen. Tijdens het opschalen van het aantal robots zal er dus een verschuiving plaatsvinden in verantwoordelijkheid, indien mensen ook daadwerkelijk worden vervangen door robots. Het onderhoud van de robots komt in handen van maar een paar werknemers. Businesscontinuïteit komt dus in het gedrang.

R3 Systematische fouten

Waar voorheen een organisatie zich moest bekommeren om menselijke fouten is dit verleden tijd in de wereld van robots. Echter, als robots een fout maken is dit meteen systematisch en kan deze fout zich snel verspreiden door de hele organisatie, aangezien de robots vaak toegang hebben tot (in verbinding staan met) meerdere systemen. De fout is systematisch omdat het in essentie een falende business rule is, die constant wordt herhaald. Ondanks dat COBIT voorschrijft dat organisaties in staat moeten zijn te kunnen reageren op eventuele onverwachte fouten, wordt dit een andere zaak in het geval van RPA. Is een organisatie bijvoorbeeld in staat

om transacties terug te draaien als het om grote volumes gaat? Kan een organisatie traceren welke robot welke fout heeft gemaakt en deze meteen uitzetten?

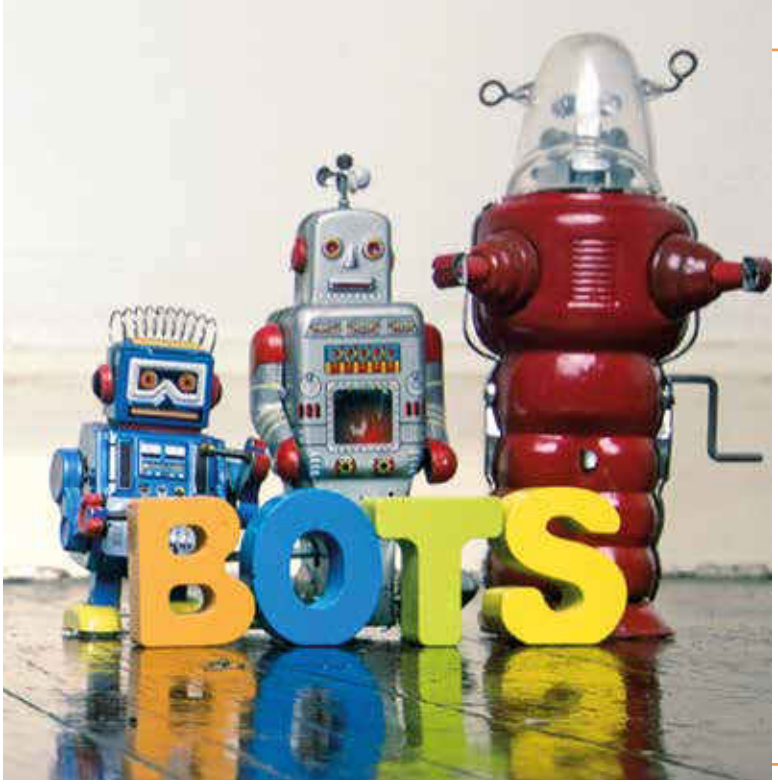
R4 Toegang
In de meeste gevallen zullen robots toegang hebben tot meerdere systemen en werken met verhoogde rechten. Robots maken gebruik van inloggegevens. Met als gevolg dat iedereen die toegang heeft tot de robots ook toegang heeft tot alle systemen in kwestie. Hier komt nog bovenop dat, gezien de selectors zo gevoelig zijn voor de zichtbare elementen op een UI, de robots in de productieomgeving vaak nog aangepast moeten worden. Dat zou betekenen dat iedereen die toegang tot de robots heeft ook inloggegevens heeft tot systemen in de productieomgeving. COBIT adresseert dit punt, maar de implicaties voor RPA zijn verstrekkender omdat de inloggegevens nu ook in handen kunnen komen van iedereen die toegang heeft tot de robots.

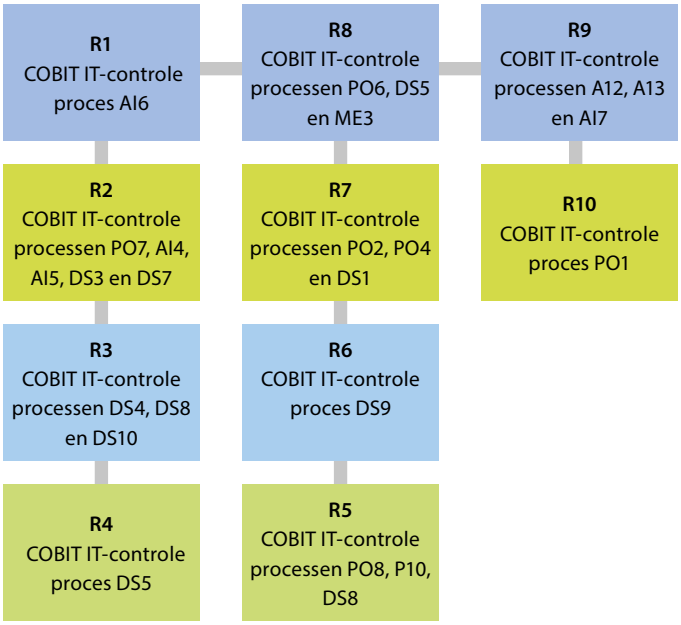
R5 Monitoring
Omdat robots relatief makkelijk gebouwd kunnen worden en in de organisatie verschillende plekken zijn waar ze van pas kunnen komen, zoals operationele, financiële of andere processen, is het niet ondenkbaar dat ze verspreid door de organisatie beheerd worden. Hoe blijft een organisatie in dit geval in staat om de operationele effectiviteit van de robots te monitoren?

R6 Kwaliteit van de code
De ene robot is de andere niet. Er is veel keuzevrijheid in het bouwen van robots. Zo kunnen twee robots dezelfde resultaten genereren maar geheel anders zijn gebouwd. Een voorbeeld is dat in de ene robot alle activiteiten betekenisvolle namen hebben gekregen maar in de ander niet. Het ontbreken van naamconventies kan leiden tot moeilijk onderhoudbare robots, aangezien er geen herleidbare structuur is waardoor veranderingen makkelijk doorgevoerd kunnen worden. Kortom, het is essentieel dat ook voor het bouwen van de robots een kwaliteitsstandaard wordt opgelegd die vooral rondom begrippen als flexibiliteit, leesbaarheid, onderhoudbaarheid en betrouwbaarheid duidelijkheid verschaffen.

R7 Compliance
De robots kunnen ook te maken hebben met (privacy)-gevoelige informatie. Ondanks dat het robots zijn, betekent dit nog niet dat zij zich niet moeten houden aan bepaalde wet- of regelgeving. Achter de identiteit van een robot gaan personen schuil die verantwoordelijk gesteld moeten kunnen worden. COBIT adresseert dit, maar als er decentraal door de organisatie vele robots actief zijn, hoe weet men dan zeker dat aan alle wet- een regelgeving wordt voldaan?

R8 Selecteren en prioriteren van robots
Het selecteren en prioriteren van de juiste robottoepassingen is een kunst op zich. Enerzijds moet door de business rekening gehouden worden met de kwaliteit en continuïteit van het proces door bijvoorbeeld zeker te weten dat het te robotiseren proces gestandaardiseerd is en niet snel gaat





Figuur 1. RPA-risico's en COBIT

veranderen. Anderzijds moet er rekening gehouden worden met technische beheersing (bijvoorbeeld onderhoud, updates en authenticatie). Het zo vroeg mogelijk starten van het gesprek tussen IT en de business is essentieel en kan vooral in een later stadium een hoop kosten besparen.

R9 In productie brengen van robots

Bijzonder aan de RPA-technologie is dat robots ook gebouwd kunnen worden door niet-programmeurs. Echter, als diezelfde mensen ook de robots in productie brengen of geen adequate testomgeving tot hun beschikking hebben, kan dit verstrekkende gevolgen hebben. Dit wordt geadresseerd in COBIT maar het is een uitdaging voor IT om een testomgeving te bouwen die een exacte replica is van de productieomgeving, aangezien de robots gebruikmaken van de UI en dus ook de verbanden tussen de systemen weten na te bootsen.

R10 Onduidelijke rollen en verantwoordelijkheden

Onduidelijkheid rondom de rollen en verantwoordelijkheid aangaande een RPA-programma is iets wat veel voorkomt. Taken die traditioneel bij IT zijn belegd verschuiven naar de business, omdat daar vaak de initiatieven worden ontplooid. Typische rollen rondom het in kaart brengen van de te robotiseren processen zijn bouwen, onderhouden, continuïteit waarborgen en monitoren.

Risicoanalyse op implementatie

Als laatste is het belangrijk te onderstrepen dat als onderdeel van COBIT (IT-controle proces PO9) een volledige risicoanalyse moet worden uitgevoerd op, in dit geval, het implementeren van een RPA-programma. Deze analyse zou de RPA-specifieke risico's boven tafel moeten krijgen, zodat de overwegingen en impact op de interne beheersing worden doorgevoerd binnen de verschillende IT-controleprocessen. Echter, uit de ervaring opgedaan door PwC tijdens het auditen van robots (binnen een COBIT context) blijkt dat, omdat RPA nog redelijk onbekend terrein is, de RPA-specifieke risico's onvoldoende geïdentificeerd worden en COBIT dus niet in staat is IT en business dichter bij elkaar te brengen. In *figuur 1* is weergegeven welke RPA-risico's, worden gemitigeerd door de COBIT IT-controleprocessen. De kleuren van de blokken geven aan in welke mate COBIT het betreffende risico mitigeert (groen: volledig, blauw: met kanttekeningen). De verschillende COBIT IT-controleprocessen hebben allemaal een uitgebreide beschrijving omtrent de activiteiten die uitgevoerd dienen te worden en de bijbehorende monitoringactiviteiten. Dit geeft internal auditors de juiste richtlijnen en handvatten om een RPA-audit uit te kunnen voeren met in het achterhoofd de hiervoor genoemde risico's.

Samenvattend is er dus een belangrijke taak toevertrouwd, nu en in de toekomst, aan internal auditors. Waarin de interne beheersing rondom robots essentieel is en de samenwerking tussen IT en de business nog nooit zo belangrijk was. COBIT geeft goede handvatten om dit te bewerkstelligen, maar dient zorgvuldig in het licht van deze nieuwe technologie te worden bestudeerd en aangevuld waar nodig. <<

Noot

1. In dit artikel wordt gerefereerd aan COBIT 4.1, aangezien COBIT 5.0 nog niet eenzelfde wijdverspreide dekking heeft in de praktijk.

Steven Boekhoudt MSc werkt als data-analist en auditor bij PwC Assurance. Hij is gespecialiseerd als RPA developer.
steven.boekhoudt@pwc.com