Versie 1.0 januari 2021
“Publieke” one-pager

NOREA | Robotic Process Automation (RPA)

RPA is naast AI en Blockchain een belangrijke ontwikkeling op het gebied van procesoptimalisatie. RPA houdt in dat een stukje software, een ‘software-robot‘, via de Graphical User Interface (GUI) vooraf gedefinieerde handelingen op IT-systemen uitvoert. Dit zijn meestal repeterende handmatige activiteiten voor data-invoer en controle. Ze doen hun werk net zoals mensen dat zouden doen en worden daarom ook wel ‘virtuele medewerkers’ genoemd. De software-robots kunnen bijvoorbeeld inloggen op applicaties, op buttons klikken en gegevens van het ene systeem naar het andere overbrengen. Met RPA leg je als het ware een extra softwarelaag over de bestaande IT-systemen heen. Deze laag bestaat uit een RPA-platform, dat de ontwikkeling en het gebruik van software-robots mogelijk maakt.

Procesoptimalisatie
Organisaties kunnen met RPA hun processen verder optimaliseren zonder hun bestaande IT-systemen aan te passen. De software-robots worden geconfigureerd met low code. Dit betekent dat na een korte training en beperkte programmeerkennis, medewerkers van afdelingen in de business zelf in staat zijn software-robots te ontwikkelen. RPA maakt het mogelijk eenvoudige maar tijdsintensieve handelingen uit te besteden aan de robot die 24/7 kan werken. Tegelijkertijd verbetert de kwaliteit van repeterende taken door eliminatie van menselijke fouten. Ook wordt het werk interessanter voor de medewerkers omdat ze zich kunnen beperken tot meer uitdagende taken.

In de praktijk lastig
In de praktijk maakt RPA de beloftes vaak niet waar. Dit komt doordat RPA-oplossingen doorgaans beperkt blijven tot automatisering van de meest eenvoudige invoertaken. Ook maakt de RPA-softwarelaag het vaak complexe IT-landschap extra lastig te beheren.

Vier vuistregels
1. Regel zowel de verantwoordelijkheid voor het beheer van het RPA-platform als de verantwoordelijkheid voor de daarop gebouwde software-robots. Beleg deze voor het platform en de robots bij de IT-afdeling (of een IT-expertisecentrum in de business) respectievelijk de lijnafdelingen, en zorg voor samenwerking tussen die afdelingen.
2. Voer risicoanalyses uit op zowel RPA-platform als individuele software-robots.
3. Stel een lifecycle-plan op per (logische groep van) robot(s).
4. Richt controls in voor het beheer van toegangsrechten voor robots.

De bij NOREA geregistreerde IT-auditors zijn onafhankelijk opererende IT-auditdeskundigen die bij organisaties de juiste opzet, implementatie en werking van een RPA-platform en de daarop gebouwde software-robots kunnen beoordelen.

NOREA | Robotic Process Automation

RPA biedt vooral voordelen bij organisaties met een omvangrijk en versnipperd IT-landschap, waar veel handmatige en repeterende data-invoer en controle-activiteiten worden uitgevoerd. Buiten de reguliere IT-afdeling om en zonder aanpassing van de onderliggende IT-systemen (‘legacy’), zijn afdelingen in de business in staat IT-oplossingen te realiseren in de vorm van software-robots, ook wel ‘virtuele medewerkers’ genoemd. De vraag daarbij is of de business capabel genoeg is om alle IT-risico’s te onderkennen en te beheersen, en of de IT-afdeling met haar expertise en kwaliteitsprocedures voldoende is aangehaakt. Ga er niet automatisch van uit, maar stel vast of dit daadwerkelijk het geval is. Laat je verder niet geruststellen door de veronderstelling dat software-robots alleen doen waarvoor ze zijn bedoeld. Het juist, volledig en veilig configureren en het monitoren van de robots blijft mensenwerk.

Van een professionele gedigitaliseerde organisatie mag je verwachten dat de kwaliteit van RPA is geborgd door:

- Duidelijke, bekendgemaakte verantwoordelijkheden voor zowel het RPA-platform als voor de daarop gebouwde software-robots bijvoorbeeld bij de IT-afdeling (of een IT-expertisecentrum in de business) respectievelijk bij de lijnafdelingen, inclusief de samenwerking tussen de afdelingen en het gebruik van (IT)procesbeschrijvingen en hulpmiddelen.
- Risicoanalyses op het RPA-platform en per individuele robot.
- Een lifecycle-plan voor elke (logische groep van) RPA-oplossing(en) waarbij software-robots worden doorontwikkeld en/of vervangen door inbouw van de robot-functionaliteit in de onderliggende IT-systemen.
- Controls voor specifieke RPA-risico’s, zoals het beheer van de wachtwoorden van de software-robots, naast generieke IT-risico’s en bijbehorende IT-General Controls.

Van een professionele gedigitaliseerde organisatie mag worden verwacht dat zij RPA op een beheerste manier inzet. Vier key aspecten:

1. Governance inclusief samenwerking met IT-afdeling

De meest vernieuwende eigenschap van RPA is dat het afdelingen in de business in staat stelt zelf, buiten de IT- afdeling om, software-robots te bouwen. De uitvoering van IT-beheersmaatregelen voor RPA verschuift daarmee deels van de IT-afdeling naar de business. Dat vraagt om een governance waarin verantwoordelijkheden zijn belegd, zowel voor het RPA-platform als voor de software-robots . Daarnaast is het nodig de (IT)-procesbeschrijvingen en hulpmiddelen voor RPA in hun onderlinge samenhang op te stellen en laten aansluiten op de standaarden van de IT-afdeling.

Voorbeeld van een audit op governance inclusief samenwerking met de IT-afdeling, is een RPA-volwassenheidsassessment van de organisatie, bijvoorbeeld via het Mindtree-automation-maturity-model. Doel is vast te stellen of het kwaliteitsniveau van de controleomgeving aansluit bij de volwassenheids-fase van de reeds geïmplementeerde RPA.

2. Risicoanalyses op RPA-platform en individuele software-robots

De introductie van een RPA-platform waarop individuele software-robots worden gebouwd, biedt kansen voor de herinrichting van bedrijfsprocessen maar brengt ook risico’s met zich mee. Om de juiste keuze te maken voor de in te richten controls, is voorafgaand aan het bouwen een risicoanalyse nodig. Deze risicoanalyse vindt plaats op zowel het platform t.b.v. non functional controls als het te robotiseren proces t.b.v. non functional- en functional controls. De risicoanalyse op het te robotiseren proces moet ook uitwijzen welke afdeling in de business eindverantwoordelijk is voor de inputcontroles, procesgerelateerde goedkeuringen en afwijkingenanalyses.

Een voorbeeld van een audit naar de betrouwbaarheid van gerobotiseerde processen is de beoordeling van IT-risico’s van het RPA-platform. Een ander voorbeeld is de beoordeling van IT-risico’s en/of functionele werking (Completeness & Accuracy) van een individuele robot.

3. RPA en Lifecycle management

Na een succesvolle pilot kiest een organisatie er vaak voor om eenvoudigweg software-robots te gaan bouwen. Gewoon omdat het kán, zonder naar alternatieven te kijken. De robot als snelle IT-oplossing staat in die gevallen centraal en er is minder aandacht voor een definitieve oplossing van het onderliggende probleem. Daarom moet niet worden nagelaten, na de implementatie elke software-robot stapsgewijs door te ontwikkelen of te vervangen door een meer structurele inbedding van de gebouwde functionaliteit in de onderliggende IT-systemen. De RPA-oplossingen periodiek beoordelen en planmatig doorontwikkelen via hetzelfde lifecycle-management proces dat bij de reguliere IT-systemen wordt toegepast, helpt het succes van RPA te vergroten.

Een voorbeeld van een audit naar RPA en Lifecycle management is een onderzoek naar de inrichting en periodieke beoordeling van de lifecycle van software-robots van een afdeling of business unit, bijvoorbeeld met COBIT, ITIL/ASL of BiSL.

4. Beheer van toegangsrechten software-robots

Een nieuwe robot heeft toegangsrechten nodig om aan te loggen op diverse IT-systemen in het gerobotiseerde proces. Belangrijke vragen zijn hoe deze toegangsrechten worden verstrekt, wat de naamgevingsconventie is, wie de verantwoordelijk manager is en hoe gebruikersnaam en wachtwoord worden beheerd. Een software-robot gedraagt zich als een IT-systeem in het klein, maar bevindt zich in de IT-stack op het hoogste niveau: dat van de GUI, en krijgt toegangsrechten als een reguliere gebruiker. Bij RPA zijn daarom op de robotgebruikersaccounts ook de standaard medewerker gerichte controls nodig, zoals identificatie, authenticatie, autorisatie/ toegangsbeveiliging en beheer functioneel user account.

Daarnaast kan de controletechnische functiescheiding in het gerobotiseerde proces anders worden ingericht, waarbij de software-robot veel meer rechten kan krijgen. Uit de risicoanalyse van het te robotiseren proces moet blijken of dit mogelijk is.

Een voorbeeld van een audit op toegangsrechten is een onderzoek naar de precieze gedragingen van een software-robot via een nadere analyse van de loggegevens van de activiteiten door de robots. De eindverantwoordelijke afdeling kan dit via data-analyse of proces mining onderzoeken.