NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Best Practices
RPA

April 2022

Deelnemers werkgroep

Eddy van der Geest RE RA (voorzitter)
ing. Amanda Feuerberg RE
drs. Els Franken RA EMITA
drs. Ricardo Krab RE
ing. Beert Kuiken RE RA
drs. Jeroen Machielse EMITA MPC CPC
drs. Miranda Pirkovski RA EMITA
drs. Alex van der Harst RE (linking pin bestuur)

Coördinatie en redactie

Postbus 7984, 1008 AD Amsterdam
Telefoon: +31-20-3010380
e-mail: norea@norea.nl
www.norea.nl

Versie Beheer		
Versie	Datum	Wijzigingen
1.0	April 2022	

Inhoud

Introductie

De afgelopen jaren is het gebruik van Robotgestuurde procesautomatisering ofwel Robotic Process Automation (RPA) aanzienlijk gegroeid.

RPA is een techniek die gebruikt wordt voor het verder automatiseren van bedrijfsvoering- en financiële processen met behulp van zogenaamde 'software-robots'[1]. RPA is gericht op het automatiseren via de user interface en/of API's (Application Programming Interface) waar mogelijk. Het is een IT-oplossing die fysieke handelingen binnen processen nabootst; een software-robot, ook wel "virtuele medewerker" genoemd, die vooral eenvoudige, repeterende taken van medewerkers vervangt. De medewerker hoeft geen saaie/routinematige taken meer uit te voeren zoals het overzetten van gegevens van de ene applicatie naar een andere applicatie. Er wordt hierbij als het ware "een softwarelaag" over de bestaande systemen heen gelegd.

Innovatiekracht

Een kenmerk van RPA is dat een organisatie eerst op kleine schaal/met weinig risico kan ontdekken wat de mogelijkheden zijn voordat ze gaat opschalen in het aantal toepassingen. De implementatie-aanpak is iteratief en kenmerkt zich door trial-error enerzijds en ontwikkelen anderzijds[2]. Het kan hierdoor het innovatievermogen van een organisatie als geheel verhogen. Het ontwikkelen van RPA vanuit het innovatieproces van de organisatie waarbij 'vrijheid' centraal staat (bijvoorbeeld via een fieldlab of learning lab) is een aanbeveling[3]. Op deze wijze kan experimenteel ervaring met RPA worden opgedaan. Er kan gebruik worden gemaakt van bijvoorbeeld een Proof of Concept (POC) om te zien of RPA in het huidige applicatielandschap kan werken. Bij de definitieve keuze van een leverancier dient men rekening te houden met de POC-resultaten en de mate waarin de ontwikkel-'vrijheid' centraal staat. Kortom: RPA met een iteratieve aanpak zorgt ervoor dat het model van ontwikkelen van proces automatisering verandert.

Risicobeheersing en verhogen effectiviteit

Bedrijfsprocessen worden steeds meer geautomatiseerd waardoor het risicoprofiel van systemen, applicaties en processen wijzigt. Echter bij een nadere beschouwing kan worden vastgesteld dat een organisatie bij toepassing van RPA zowel vanuit risico perspectief als vanuit het perspectief van effectiviteit rekening moet houden met randvoorwaarden. Het voordeel dat RPA kan bieden door vervanging van de vele handmatige rule based takenin organisaties met een omvangrijk en divers IT-landschap, wordt tenietgedaan als RPA niet structureel is ingebed in de organisatie. Eén van de valkuilen is dat afdelingen zelf aan de slag gaan met RPA zonder

1 Wikipedia: https://nl.wikipedia.org/wiki/Robotgestuurde_procesautomatisering

2 in een OTA-omgeving waarin de scheiding tussen test en productie omgeving zijn gescheiden.

3 'How to Build data literacy in your company' (Febr. 2021) MIT Management SLOAN School

dat verschillende kennisgebieden betrokken worden of hiërarchie is ingebed. Met andere woorden dient er vooreerst een deugdelijke governance rondom de inzet van RPA te worden opgezet.

Opzet en doel van de best practices

Inzet van nieuwe IT tools brengt andere en nieuwe risico's met zich mee. De NOREA werkgroep RPA heeft daarom een set van 'best practices' ontwikkeld waarin op basis van risico inschatting specifieke aandachtspunten zijn opgenomen indien een organisatie overweegt RPA te implementeren of heeft geïmplementeerd. De set van best practices richt zicht niet alléén op het beheersen van risico's maar ook op het stimuleren van een lerende organisatie door bijsturing vorm te geven ten behoeve van het management. Dit is zichtbaar doordat de Plan-Do-Check-Act-cyclus van Deming (hierna: PDCA) aan de opzet is toegevoegd. Per onderdeel worden aandachtspunten met organisatie-impact vermeld en bijpassende beheersmaatregelen.

Het doel van de best practices is enerzijds om organisaties handvatten te bieden bij het implementeren van RPA, risico's te beheersen en het innovatievermogen binnen organisaties te stimuleren. Anderzijds is het doel om IT-auditors en financial auditors handvatten te bieden voor het auditen van RPA. De best practices kunnen in combinatie met standaard ITGC-frameworks gebruikt worden.

Disclaimer: deze set van best practices vermeldt niet alomvattend alle risico's. Daarnaast zullen voor de lezer enkele aandachtspunten herkenbaar zijn als een generiek (IT-service proces) risico zoals bijvoorbeeld autorisatiebeheer of change management. De werkgroep heeft op basis van literatuur en praktijkervaringen de RPA specifieke risico's ten aanzien van een RPA implementatie geïnventariseerd en benoemd als aandachtspunt.

Tot slot

De werkgroep ziet dit als een dynamisch document, ook gezien de te verwachten ontwikkelingen op RPA-gebied. Hierbij valt te denken aan het combineren van RPA met AI, blockchain, chat bots en machine learning (Hyper automation). Ze zal eind 2023 evalueren op welke punten de best practises aangescherpt kunnen worden en de Check & Act van de Deming cyclus verder uitwerken. Voor vragen of suggesties kunt u contact opnemen met norea@norea.nl.

Best Practices RPA

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
1	**Plan**	**Strategische sturing** (Planvorming)	Bedrijfsstrategie en afdelingsdoelen worden niet behaald omdat het ontbreekt aan draagvlak en afstemming tussen afdelingen over RPA of het wel implementeren van RPA maar zonder centrale regie Het gevolg kan zijn dat RPA niet juist, volledig of tijdig wordt geïmplementeerd waardoor de organisatie blootgesteld wordt aan financiële risico's en/of kansen niet worden benut. Ook zorgt dit voor een minder efficiënte manier van werken.	Waarborgen dat verschillende partijen (zoals bijvoorbeeld risk management, externe accountant etc.) voldoende kennis/inzicht hebben in de toepassing van RPA binnen de onderneming waardoor draagvlak op het hoogste hiërarchische niveau ontstaat bij de uitrol van RPA (waaronder de CTO of CIO). Het organiseren van trainingen, kennis-sessies en workshops om inzicht en draagvlak te creëren	Door onbekendheid en het innovatieve karakter van RPA binnen o.a. het hoger management wordt implementatie soms bewust of onbewust vertraagd. Tone-at-the-top om de perceptie ten aanzien van RPA positief te beïnvloeden, verhoogt de kans op het draagvlak binnen de organisatie.
2	**Plan**	**Governance RPA** (Inrichten besturingsmodel en eigenaarschap)	Het onjuist en onvolledig inrichten en implementeren van de taken, verantwoordelijkheden en bevoegdheden binnen de organisatie kan leiden tot verminderd eigenaarschap waardoor de RPA implementatie- en beheeractiviteiten onjuist of niet tijdig worden uitgevoerd. Dit zet de realisatie van de bedrijfsdoelen met RPA onder druk.	Opzetten van een governance - of besturings-model waarin taken, verantwoordelijkheden en bevoegdheden zijn belegd inclusief de overlegstructuren passend bij de fase van ontwikkeling (volwassenheid). Operationeel maken en implementeren van stakeholdermanagement op basis van juiste selectie stakeholders o.b.v. invloed en impact. Beleg het eigenaarschap en wijs de verant-woordelijkheden van het RPA platform toe binnen de organisatie. Richt overleg-structuren in en zorg voor vastlegging van de overleggen.	Business / IT alignment en onderlinge aansluiting tussen gebruikers en IT afdeling (en security). Een belangrijk kenmerk van RPA is dat de business in de lead is. De regierol van de business mag de samenwerking niet belemmeren. De RPA bot kan je zien als een virtuele medewerker met één verantwoordelijke manager/'eigenaar'. Deze manager is verantwoordelijk voor de inhoud van het RPA-script en het juist en tijdig verwerken van uitval (afhandeling van uitzonderingen) nadat het script heeft gedraaid (virtuele medewerker heeft zijn werk gedaan).

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
3	**Plan**	**Leverancier selectie** (gericht op RPA-partnership)	Het leverancierselectie proces wordt onjuist en niet tijdig gevolgd waardoor er geen goede keuze wordt gemaakt voor het RPA software pakket met als gevolg 'vendor lock-in'. Dit kan leiden tot een financieel risico. Daarnaast is ook het selecteren van je (juiste) implementatiepartner en afspraken daarmee maken een risico. Indien de implementatiepartners het intellectueel eigendom op scripts claimen loopt de organisatie een continuïteitsrisico als scripts meegenomen kunnen worden nadat een contract is beëindigd. Intellectueel eigendom van scripts dient bij de organisatie te liggen.	Toepassen van een standaard pakket-selectie proces of standaard aanbestedingsprocedure met vooraf gecommuniceerde regels met specifiek aandacht voor RPA eisen. 1. Identificeren en definiëren minimale (beveiligings)standaarden voor uitrol RPA op het platform. 2. Passende leverancier die trusted partner wordt voor de RPA oplossingen met aandacht voor: bestendigheid in de toekomst, strategie m.b.t. vendor lock-in - exit strategie, overdraagbaarheid code. 3. Tijdens de pilotfase, maar ook daarna richten op partnership. 4. Het contractueel nalopen / challengen van clausules in de overeenkomst met de implementatiepartner. 5. Intellectueel eigendom van ontwikkelde scripts contractueel afdwingen en voorkomen dat vendor lockin ontstaat met de implementatie partner.	De RPA software keuze is afhankelijk van het bestaande IT-landschap. Na het onderzoek van de requirements kan een RPA bot prototype worden ontwikkeld, dat in een pilotfase of pilotstudie onderzocht wordt op praktische toepasbaarheid. RPA initiatieven worden veelal enthousiast gestart zonder vooraf gedefinieerde (beveiligings)eisen en wensen. Soms zijn betrokken externe consultants gelieerd aan een bepaalde RPA leverancier en wordt te weinig aandacht besteed aan de bestaande IT- infrastructuur en afhankelijkheden binnen het IT-landschap.
4	**Plan**	**Life cycle management** (LCM, zowel RPA	Het RPA software pakket en aanpalende IT-systemen en -infrastructuur zijn aan (onderlinge) technologische en security	Houdt rekening met een ontwerp filosofie[4] waarbij elke RPA bot volgens dezelfde	Voor RPA geldt: tijdig inspelen op interne en externe veranderingen.

[4] Voor meer informatie: https://www.ey.com/en_gl/consulting/five-design-principles-to-help-build-confidence-in-rpa-implement

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
		bots als RPA platform)	veranderingen onderhevig waardoor aandacht voor LCM is vereist. Bij het niet juist, volledig of tijdig doorlopen van de LCM cyclus, kan een continuïteit- en financieel risico ontstaan.	uitgangspunten (design priciples) wordt gebouwd. Implementatie van onderhoudsplannen en actualiseren van de dienst, RPA bots (inclusief aandacht voor platform, performance virtuele medewerker, code review).	Als voorbeelden kunnen worden genoemd de integratie met AI of het IT landschap dat aan veranderingen onderhevig is (te lang doorgaan met verkeerde/verouderde RPA-platformen). Het is ook van belang goed op de hoogte te zijn van de IT lifecycle om zo tijdig aan te haken op testperiodes van nieuwe releases van applicatie om de huidige RPA bedrijfsvoering te behouden tijdens updates. Mocht dit niet gebeuren dan kan de business niet rekenen op de virtuele medewerkers.
5	**Plan**	**RPA kennis en overdracht** (Personeelsbeleid, opleidingen en training)	Onvoldoende kennis van RPA kan leiden tot onbetrouwbare ontwikkeling (met name change/incidentmanagement) en implementatie van RPA bots met financiële- en continuïteitsrisico's als gevolg.	Trainen van personeel en lijnmanagement. Het tijdig opleiden van betrokken medewerkers bij gebruik en ontwikkelen van RPA platform inclusief de RPA bots. Certificeren van de werknemers betrokken bij ontwikkeling van RPA bots. Organiseren van periodieke robotica kennis-sessies (netwerk en kennisdeling).	De business is meestal in de lead is bij RPA-oplossingen. Voldoende IT kennis en vaardigheid bij het bouwen van bots is alsnog veelal vereist bij RPA. Dit kan een kritische succesfactor zijn. Ook is er een wijziging in de activiteiten van de medewerkers. Hoe kan je uitval van de virtuele medewerkers lezen, verwerken en zorgen dat het proces tijdig is afgerond. In dit onderdeel zit ook een grote management veranderopgave.
6a	**Plan**	**Risico identificatie**	RPA bots voeren handelingen uit waarvoor de risico's niet zijn onderkend met continuïteit- en integriteitsrisico's als gevolg.	Plan en implementeer risk assessments, BIA's en PIA's inclusief beheersmaatregelen. Ontwerp een PDD (proces design document) waarin zowel de handmatige werkwijze van	RPA kan worden gebruikt om arbeidsintensieve werkzaamheden te verrichten en medewerkers te ontlasten. Bij calamiteiten bestaat het risico dat

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
			Risico's zitten daarbij o.a. in: • Ongeautoriseerde toegang tot systemen. • Doorbreken van functiescheiding bij transactieverwerking door de RPA bot. • Eventuele omgang met persoonsgegevens en toegang daartoe. • Gebrek aan eigenaarschap in de business voor automatiseringsdoelstelling.	de medewerkers als de toekomstige werkwijze van de robot uitgewerkt is. Bij uitval kunnen de medewerkers altijd deze instructie volgen. Benoem een eigenaar voor elke bot.	medewerkers met kennis en vaardigheden niet meer beschikbaar zijn of dat medewerkers niet eenvoudig de werkzaamheden van een bot kunnen overnemen.
6b	**Plan**	**Risico identificatie** (RPA platform)	RPA platform onvoldoende veilig: • Ongeautoriseerde toegang tot het platform. • Onvoldoende functiescheiding in rollen en verantwoordelijkheden binnen het platform. • Toegang tot de logging.	Plan en implementeer (security) risk assessments, BIA's en PIA's inclusief beheersmaatregelen, gebaseerd op standaarden en best practises voor het RPA platform.	Voldoen aan de minimale security baseline.
7	**Do**	**Platform realisatie** (Infrastructuur)	RPA platform en RPA bots zijn geïmple-menteerd zonder rekening te houden met de requirements, technische- en security standaarden uit de (bestaande) IT Architectuur van de organisatie. RPA als losse applicatie implementeren leidt tot inefficiëntie en minder kostenbeheersing. Het kan ook leiden tot integriteit en beschikbaarheidsrisico's.	Beheren van het platform en afstemmen met onderliggende bestaande infrastructuur indoor Technisch Beheer/Applicatie Beheer van de IT afdeling (of DevOps Teams).	

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
8	**Do**	**Ontwerpen rollen en autorisaties** (Creëren en implementeren toegangsrechten RPA bots)	Rollen van de RPA bot zijn niet juist, volledig of tijdig gecreëerd en/of geïmple-menteerd met als gevolg dat de RPA bots te ruime bevoegdheden krijgen. Hierdoor kan een fraude-, integriteit en/of privacy risico ontstaan.	RPA bots krijgen toegangsrechten gebaseerd op reguliere toegangsprofielen net als reguliere medewerkers (dus geen beheeraccount) rekening houdend met functiescheiding en het need-to-know-principe. Er zijn procedures opgesteld en geïmplementeerd om de rollen te beheersen. De naleving wordt getoetst (zoals ook geldt voor een 'gewone' gebruiker).	Need-to-know gebruik van persoonlijke data principe wordt ook bij de ontwikkeling van RPA bots toegepast en alleen noodzakelijke persoonlijke gegevens worden opgenomen in het transactieverslag van de bot. Hetzelfde geldt ook voor financiële gegevens en/of kritische bedrijfsgegevens.
9	**Do**	**Autorisatiebeheer** (Toekennen, muteren en intrekken toegangsrechten RPA bots)	Toegangsrechten worden niet juist, volledig of tijdig toebedeeld aan de RPA bot of medewerkers (incl. leverancier) die over RPA bot credentials beschikken. Dit kan leiden tot ongeautoriseerde toegang tot data. Hierdoor kan o.a. een fraude- en/of privacy risico ontstaan. Toegangsrechten naar IT systemen aangemaakt t.b.v. de RPA bots kunnen misbruikt worden door andere RPA bots en/of medewerkers.	Credentials van RPA bots of toegangsrechten worden beheerd door de afdeling verantwoordelijk voor de betreffende RPA bot. Koppel de RPA bot-ID aan de bestaande medewerkers rollen. Er zijn procedures opgesteld en geïmplementeerd om de toegangsrechten te beheersen. De naleving wordt getoetst. Voor de enveloppenprocedure (Zie punt 11. Beheren speciale toegangsrechten).	Een RPA bot dient te worden benaderd als een 'virtuele medewerker'. Hiervoor gelden dezelfde normen ten aanzien van het toekennen, muteren of intrekken van autorisaties. (Autorisatiebeheer o.b.v. ITIL). Goed gebruik is om in de naamgeving zichtbaar te maken dat de betreffende user een RPA bot is. Autorisatiebeheer en de risico's heb je effectief op vier niveaus: • Toegang tot de RPA applicatie • Toegang tot Active Directory (AD-niveau) • Toegang tot de doelapplicaties • Toegang tot locatie van inputdata van robots (i.e. wanneer bijvoorbeeld de inputdata van een robot op een lokale schijf staat en die vrij toegankelijk is)

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
					Gebruik van consistente naamconventies door ontwikkelaars stimuleert standaardisatie.
10	**Do**	**Beheren speciale toegangsrechten** (Systeem admins en beheeraccounts)	Technische accounts en beheer accounts (toegangsrechten naar platform en RPA bots) worden niet voldoende beheerst met als gevolg dat een fraude-, integriteit- en/of privacy risico ontstaat.	Er zijn procedures opgesteld en geïmplementeerd om deze toegangsrechten naar RPA platform en bots te beheersen. De naleving wordt getoetst. Implementatie van een (geautomatiseerde) enveloppenprocedure waarbij de inlog- en wachtwoord-gegevens van de speciale toegangsrechten in een (digitale) kluis worden bewaard en alleen bij incidenten ter beschikking worden gesteld.	Een RPA bot is een digitale medewerker waarvoor de afdelingsmanager verantwoordelijk is. De RPA bots kunnen geen autorisaties met ruime rechten krijgen. Aandachtspunt is dat de RPA bot een eigen user account krijgt toegewezen en er geen SUPER user rechten zijn gekoppeld aan RPA bots. Belangrijk is handhaving van de bestaande functiescheiding en het vastleggen van de activiteiten van de bot met een audit trail.
11	**Do**	**Load balancing** (Beheersen keten-afhankelijkheid)	RPA bots belasten onderliggende systemen te zwaar, waardoor overige (operationele) processen worden verstoord. Dit kan leiden tot een continuïteitsrisico.	RPA bot als batchverwerker inplannen rekening houdend met belasting van de systemen door operationele processen en/of andere geautomatiseerde batchverwerkingen.	Volgtijdelijkheid binnen het RPA proces verdient aandacht, ook in aansluiting met overige batch gerelateerde verwerkingen in het landschap en back-up en recovery processen.
12	**Do**	**Vastlegging RPA-specificaties** (Documentatie RPA platform en RPA bots)	Het gerobotiseerde procesdeel is onvoldoende gedocumenteerd in technische en functionele ontwerpen met als gevolg dat bij incidenten de RPA bot niet tijdig kan worden hersteld.	Documenteer en registreer de RPA bot als een regulier IT-systeem en in over-eenstemming met standaard IT-processen en procedures zoals gehanteerd binnen de organisatie: Documentatie gaat over technisch (script van de RPA bot) en functioneel ontwerp en	Het gebruik van video/screenshots kunnen de foutopsporing ondersteunen en vereenvoudigen.

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
				inclusief een data flow diagram en GUI-toegangsrechten naar andere systemen. Een juiste en volledige CMDB-registratie en juiste en volledige changedocumentatie zoals Go Live, GAT. Tot slot inzichtelijk maken van de terugverdienratio (ROI).	
13	**Do**	**Registreren en bijhouden CMDB** (RPA gerelateerde specificaties)	Onvoldoende inzicht in de RPA specificaties bij incidenten of bij regulier onderhoud van het RPA platform met als gevolg een continuïteit risico.	Registreer de RPA bot in de CMDB zodat duidelijk is met welke applicaties/systemen de RPA bot connecties heeft. Met deze informatie kan de proceseigenaar een Business Continuity Plan opstellen.	Indien de CMDB in beheer is bij een IT afdeling en de RPA oplossing bij de business, is het verstandig om juiste afspraken te maken over de beheersing van de registratie(s) zodat alle assets inzichtelijk blijven.
14	**Do**	**Inrichting RPA OTA** (Scheiding test/acceptatie)	De OTA omgeving is onjuist ingericht met als gevolg dat er onzekerheid is dat het RPA proces betrouwbaar wordt uitgevoerd in de productie omgeving. Het gevolg is een proces- en integriteitsrisico.	Het opzetten van de test-, ontwikkel en acceptatieomgeving (OTA) die een afspiegeling is van de werkelijke RPA omgeving en het uitvoeren van een ketentest[5].	Door de schaalbaarheid van RPA behoeft dit onderdeel extra aandacht. Met RPA moet rekening worden gehouden met de verschillende applicaties en omgevingen binnen de infrastructuur. De projectmethodiek van implementatie zorgt niet direct voor een andere wijze van beheersen.

[5] Een ketentest kan worden gedefinieerd als een test waarbij een of meerdere operationele processen worden doorlopen over een aangesloten reeks van applicaties en platforms. Doel is om vast te stellen of de processen en systemen juist zijn geïntegreerd en effectief werken als één geheel.

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
15	**Do**	**Testen RPA bots** (Testen en naar productie brengen RPA bots)	RPA bots worden onjuist, onvolledig en niet tijdig getest met als gevolg dat er onzekerheid is dat het RPA proces betrouwbaar wordt uitgevoerd. Het gevolg is een proces- en integriteitsrisico.	Overzetten van de bot naar de productie omgeving rekening houdend met de keten en de afhankelijkheden. Goedkeuring vooraf en vastlegging testresultaten. Richt het vier ogenprincipe in tijdens overzetten van de bot naar productie.	Als de test en productie omgevingen gespiegeld zijn (en periodiek gecloned met productiedata) gaat dit goed, zo niet dan verwerkt RPA de items niet. Er zal in principe nooit foutieve verwerking plaatsvinden. Er is wel altijd nazorg/verwerking van uitval nodig voor bijvoorbeeld scenario's die in de testomgeving niet tegen gekomen zijn. Het is goed om eerst een kleine run in productie te doen om risico/impact in geval van fouten in de bot te beperken.
16	**Do**	**Incident management** (RPA bots)	Incidenten worden niet opgepakt, waardoor continuïteit van de RPA bots niet is gewaarborgd.	Stel incidentenmanagement (procedure) op met aandacht voor RPA. Incidenten worden gemeld aan de verantwoordelijke gebruiker (afdeling/systeemeigenaar) via het incidentenplatform. Vanuit design rekening houden met hoe uitval moeten worden afgehandeld. Benoem taken, bevoegdheden en verantwoordelijkheden (eigenaarschap benoemd in punt 2. Governance RPA) voor opvolgen van incidenten (SLA) en melden aan proceseigenaar.	Bij ontwerp en bouw dient extra rekening te worden gehouden foutafhandeling en loggen van transacties, zodat bij incidenten foutopsporing wordt vereenvoudigd.

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
				Definieer 'handmatige' fall-back procedures. Een manager moet probleemeigenaar zijn.	
17	**Check**	**Monitoren non-functionals** (RPA bots en operaties)	Onvoldoende inzicht in het door de RPA ondersteunde, operationele proces met als gevolg dat het inzicht in de effectiviteit ontbreekt. Dit kan leiden tot continuïteitsrisico en/of een financieel risico.	M.b.v. een operationeel dashboard van alle RPA bots wordt op dagbasis gemonitord of de ingeplande RPA bots (veronderstelling: inzet van RPA bots is batch-verwerking en staat niet 24/7 'aan') probleemloos gerund hebben en daarmee effectief zijn. In geval van een run-incident wordt deze afgehandeld via een incident management proces (bij voorkeur aansluitend bij het standaard incident management proces van de IT afdeling).	Een belangrijk aandachtspunt is het feit dat het initiatief vanuit de klant komt op het gebied van RPA. Incidentafhandeling heeft een relatie met de beheerorganisatie en dient gezamenlijk opgepakt te worden en de oplossing geborgd.
18a	**Check**	**Evalueren RPA-implementatie** (Strategisch / Tactisch)	(Bedrijfs) doelstellingen van RPA worden niet gehaald (waaronder procesoptimalisatie - doelen, kostenbesparing). Dit kan leiden tot een financieel of bedrijfvoeringsrisico.	Periodieke rapportering en evaluatie van RPA KPI's zoals besparingen (succes) in bespaarde uren en gerealiseerde RPA bots, in samenhang met klant- en medewerkerstevredenheid (bijv. o.b.v. enquête) en in relatie tot de gestelde doelen (zie 1. Strategische sturing).	Directie en management rapportages (evt. stuurgroep) vormen de basis voor de beheersing van dit onderdeel. Als voorbeeld kan worden benoemd: de voortgangs-rapportages RPA programma.
18b	**Check**	**Evalueren inzet RPA en risicobeheersing** (Operationeel)	Het management heeft onvoldoende inzicht in de gerobotiseerde processtappen door ketenopbouw en risicobeheersing van de bots. De keten van RPA bots is in werking onbetrouwbaar. Dit kan leiden tot een continuïteitsrisico.	Periodieke rapportering over key RPA-platform controls en key RPA bot controls (key-functionaliteit) en een evaluatie van de control testresultaten (vergelijkbaar met een beoordelingsgesprek met de virtuele medewerker).	Nadrukkelijk worden hier de operationele monitoringsrapportages over RPA bedoeld. Als voorbeelden kunnen worden genoemd: De RPA bot-inzet die veel handmatig (correctie) werk creëert verderop in de

#	PCDA	Onderwerp	Aandachtspunt met organisatie-impact	Beheersingsmaatregel	Toelichting in relatie tot RPA
					keten. Het aaneenrijgen van RPA bots kan leiden tot een domino effect bij een storing. Suboptimale proces-automatisering. Om dit inzichtelijk te maken kunnen de volgende rapporten helpen: incidenten, performance rapportages, periodieke root cause analyse aantal RPA bots live, aantal gekoppelde RPA bots etc. En daarnaast incidenten met als oorzaak RPA bot-inzet.
19	**Act**	Bijsturen RPA samenwerking en implementatie (Vanuit strategisch en operationeel niveau)	Verbetervoorstellen voor de inzet van RPA en risicobeheersing worden niet volledig, juist of tijdig opgevolgd. Hierdoor bestaat de kans dat de operationele doelen in relatie tot RPA mogelijk niet worden behaald met een financiële risico als gevolg.	Toetsing van de opvolging van de verbetervoorstellen (follow-up).	Bijsturen op alle voor genoemde risico's. Op alle onderdelen vormt dit item het sluitstuk.