The benefits from a cost perspective are clear and often form the major driver for the initial adoption of RPA – but what about the risks? | *March 2016*

Robotic Process Automation – friend or foe for your risk profile?

pwc

pwc.com.au/rpa

What is Robotic Process Automation?

Robotic Process Automation (RPA) is the automation of processes using technology and involves the use of software 'robots' that are easy to configure, require little IT expertise and can be quickly 'trained' and deployed to automate manual tasks. They differ from traditional software by working at the user interface level, replicating the exact actions a human user would take and creating, in effect, a virtual BPO.

Activities might include performing double data entry, copying and pasting data between computer systems, reconciling and cross-referencing data between different systems and implementing high-level decision making at key points along the business process.

What's new about it?

Many of the principles within RPA have had a long history, such as basic screen scraping. We are seeing increasing interest in RPA with recent advances in the underlying technologies improving stability and scalability. The RPA market has started to move beyond the basic rule based processing to RPA that taps into unstructured data and intelligence through content analytics and process automation. In an environment where there is pressure to digitise operations, RPA enables rapid implementation, delivering significant and sustainable value in short timeframes as it can be incorporated into an organisation's legacy systems and manual processes.

Who will benefit from it? And why?

Organisations of varying scale, size and structure can leverage RPA to streamline and automate specific manual processes. The benefits of improved customer experience, cost reduction and increased speed to market are clearly communicated, and increasingly supported by early adopters but there is little focus on two other potential benefits, risk reduction and improved compliance – assuming you get your RPA implementation right.

Why can't my core systems replace the manual workarounds rather than RPA?

This is a common question as RPA it is just another form of software with inbuilt rules and procedures, like any core IT system. However, RPA seeks to automate the many manual processes that a human user has to do to work around software gaps or defects that span multiple systems. These workarounds have often been created as core IT systems have been unable to keep pace with the changing business needs (e.g. regulatory requirements or new products) due to the high investment cost and time required.

In addition, the challenges of delivering IT projects often leads to implementations with lower quality as budgets and timeframes get compressed. The acceptance of manual processes to work around known software defects becomes the new normal as there is often no budget or accountability to fix these post 'go-live'. These manual workarounds continue and consume increasing resources as the business scales and needs evolve.

Automation of manual steps to mitigate risk

Regulatory and compliance requirements for businesses continue to increase. The response to meeting these requirements too often involves piecemeal IT system changes with reliance on manual workarounds to process high volumes of information. Manual entry relies on the diligence and attention to detail of often junior or low skilled employees. Failures in processing result in inaccurate data and reporting. Small errors in data quality over the past number of years have resulted in large spend on 'remediation programs' responding to increased regulatory scrutiny and interventions. However, too often the remediation effort focuses on the symptoms rather than fully addressing the root cause of the issue: the manual nature of the tasks and the natural variability in human behaviour.

The automated nature of RPA can ensure a high level of compliance. The *APRA Prudential Practice Guide* CPG 235 'Managing Data Risk' principle notes that 'automation (where viable) is used as an alternative to manual processes'. Unlike humans, who may skip a process step, or not be consistent in the processing of a transaction, the robot performs the task without bias or any variation. This gives support to the automation agenda to manage and minimise risk.

In addition, for those tasks where humans are making repetitive simple decisions based on data or criteria, RPA has the ability to perform these types of exception management tasks. Most of the time, the scenarios people are faced with to execute these exception processes are limited in quantity. As long as the decision matrices can be documented, RPA can handle them and significantly relieve the repetitive burden and risk of error from the human resources performing these tasks. Implemented correctly, RPA can support consistent application of rules and adherence to control frameworks for decision making as the robots are programmed to follow the standard operating procedure and hence perform the task in exactly the same way, every single time.

Training costs of compliance drop substantially with RPA as well, as RPA allows for precise process execution without the ongoing effort and cost of training a human workforce.

What are the regulatory considerations?

Given that RPA is an emerging technology in the service industries, there are no standards or formally agreed upon industry controls specific to RPA. Indeed, this has been given little focus to date as the drivers have been around cost reduction and the adoption has been modest to date in South East Asia.

APRA Prudential Practice Guide PPG 234 'Management of security risk in information and information technology' expects that, in a production environment, a regulated institution would only authorise the use of technologies that have matured to a state where there is a set of industry-accepted controls to manage the security of the technology.

In Australia, there are no clear standards and practices which apply to RPA. However, APRA clearly states that any software that is used for the processing and retention of critical or sensitive data needs to comply with the relevant life-cycle controls of the entity. In some ways, RPA could be viewed as a form of end-user computing. APRA notes that end-user computing for the purpose of automating day-to-day business processes creates a risk that data life-cycle controls may be inadequate given that end-user developed/configured software is not typically subject to the same controls as a technology function.

Similarly, in New Zealand there are no defined requirements around automation or the management of technology risks stipulated within the *Financial Markets Authority Act 2011* (NZ) or the *Financial Markets Conduct Regulations 2014*. The regulations note only mentions information technology in the context that IT systems and processes must be appropriate to allow the custodian (or financial institution) to meet the requirements of an assurance audit engagement and report.[1]

In Singapore, the MAS Internet Banking and Technology Risk Management Guidelines recognise the elevated level of risk which stems from technology innovations such as system virtualisation and automation. In addition to the guidelines, a number of notices have been added to the *Monetary Authority of Singapore Act 1970* (SG), providing legal requirements on how to manage the risk around implementing these technologies within financial services organisations. In particular, guidelines 6.4.2 – 6.4.4 of the *Monetary Authority of Singapore – Technology Risk Management Guidelines* specifically relate to automation and state that in deploying process automation, the financial institutions should use recovery measures, data protection and review and test configurations so as to 'ensure the integrity and reliability of the applications'.[2]

As such, it is critical to ensure that relevant control standards are deployed for the rollout and management of RPA. Whilst the RPA adoption should be business driven and led, engagement with IT and control functions is required to ensure accepted control standards are applied in the same manner as core IT systems.

What about privacy and data protection?

Privacy and Data Protection is also gaining increasing focus and attention and needs to be considered for RPA, especially if the task involves the processing of personal information. Whilst there is no RPA specific guidance or precedent within Australian privacy law around automation, *Australian Privacy Principle* (APP) 1 in the federal *Privacy Act 1988* (Cth) requires entities to take reasonable steps to implement practices, procedures and systems that will ensure privacy compliance, and this needs to be built into the RPA framework.

Similarly, for both New Zealand and Singapore there is no specific guidance around the management of automation and privacy. However, the New Zealand Privacy Commissioner recognises the heightened risk of privacy breaches that occur through technology innovations and has developed technology specific guidance for applications, digital data and the cloud. In implementing RPA, organisations will need to be compliant with the twelve information privacy principles under the *Privacy Act 1993* (NZ). Similarly, the *Singapore Personal Data Protection Act 2012* (SG) (PDPA) is not prescriptive on privacy regulations around technology. Organisations must comply with the provisions of this act in considering consent, purpose and reasonableness of data collection and use.[3] Guideline 17.5 of the *Advisory Guidelines* on key concepts in the PDPA also suggests a number of technical measures an organisation may use to protect personal data.[4]

What control standards should apply to RPA?

From our experience, a successful rollout of RPA requires consideration of the full framework, from development of a digitisation strategy; the methodology to select the right processes and prioritisation of these processes; governance approvals; development, testing and deployment; and implementing the right infrastructure, support and operating model to manage the new robotic workforce.

So what are these standards? Example questions to consider include:

Development and deployment:

- What is the overarching governance framework for adoption of RPA and alignment to risk, compliance and IT/data frameworks?
- How does RPA fit into the overall IT enterprise architecture?
- Have we selected the right processes to automate?
- Have we optimised these processes before we automate?
- How is the process integrated with up and downstream business processes and how well are these linkages known and documented?
- Have the requirements for IT disaster recovery and scalability been defined and addressed and broader resilience considered?
- Will RPA capture a complete audit trail to confirm the origin of data and provide transparency of alterations?
- Will distinct user IDs and passwords be assigned to each robot – who is accountable for management of these accounts and for the robot actions?

Ongoing support and maintenance:

- How do we manage changes to the robot configuration and any integrated up and downstream processes in a controlled manner?
- How do we ensure the robotic workforce have turned up for work – i.e. are logged in, functioning, balancing workloads and meeting SLAs? Who manages the control room?
- What is the incident management framework to respond to instances where the robotic workforce is impacted by unforeseen process changes?
- What is the support model in place for the robotic workforce and how does this tie into the organisation IT service management model?
- What user access management controls apply to the robot user – do our current processes and security policy allow for such a 'system' user?
- How do we ensure the access privileges assigned to the robot are not inappropriately used or accessed by other parties?
- Are we regularly assessing the failover and recovery capability and plans to ensure any disruption in the robotic availability does not impact the business operations?
- What is the fall back plan when the human workforce no longer know the manual steps that were previously undertaken?
- Do we regularly assess that the configuration of the rule set and processing logic remains relevant to our business needs and demands?
- What oversight and assurance over RPA deployment and use is provided across the Three Lines of Defence? How do the skills and techniques of risk and audit function need to evolve in a highly digitised environment?

So what could go wrong – what is my foe?

As outlined above, a key benefit of automation is improved compliance accuracy as the robot never deviates from the configured algorithms and business program logic programmed into the software. However, in this also lie the possible weaknesses:

- In older RPA technologies, if there is a business process change, the software may fail to perform. In order to avoid automation failures, changes will have to be planned, communicated, tested and made within a strong governance framework. However, newer platforms are able to accommodate simple changes without issue, minimising the likelihood of this risk in the future.
- Basic RPA technology is literal; it can only do what it's been told to do. In human nature, there are often innate rules that are followed without conscious thought applied, and as such there is a heightened risk of 'missing' rules in a process because the decisions just make natural sense to the human operator and so aren't documented. More advanced RPA is starting to incorporate elements of Artificial Intelligence but it will some years before it is expected to reach this level of maturity.
- If the processes are not mapped correctly, automated activities may be incorrectly performed or incomplete. Automating an inefficient or poorly controlled process only amplifies the issue.
- RPA may avoid the core issue of the need for underlying process transformation. Given its relative low cost and complexity, organisations may be seduced by an RPA tactical fix rather than addressing the root cause and tackling process changes.
- The downside of human processing is the variability in quality and risk of human processing error. However, there is a natural safeguard in that there are many transactions and many users, meaning that errors will often not be systemic or widespread across the business process or data set. With automation, there is consistency in application. So if you get it wrong, you consistently get it wrong and therefore the risk is that any error becomes a systemic and widespread issue across that business process and data set. It's all your eggs in one basket approach (or robot configuration).

How do we know it's working as intended?

Despite rigorous testing prior to deployment, it is only from seeing the robot live in processing that you may uncover the unknowns in the production environment. Therefore, there is a need at the post-deployment stage to review the processing and decisions made by the robot to ensure they align with expectations. This should be done early in deployment to allow for any correction of rules and logic to be applied.

The PwC Process Intelligence tool is an automated way to visualise where every transaction occurs in a process, identify process inefficiencies, bottlenecks, control and data quality issues and identify to what extent transactions follow the expected paths versus the actual paths.

Early consideration of governance, risk and assurance is important to making RPA your friend

As the adoption of RPA shifts from proof of concept, trial projects to enterprise programs across financial institutions, the industry will need to agree upon standards for governance, risk and assurance. As we have seen from cloud implementations, the key to realising the business of benefits RPA is ensuring early regulator engagement and a plan to demonstrate sound governance and risk management over regulated data.

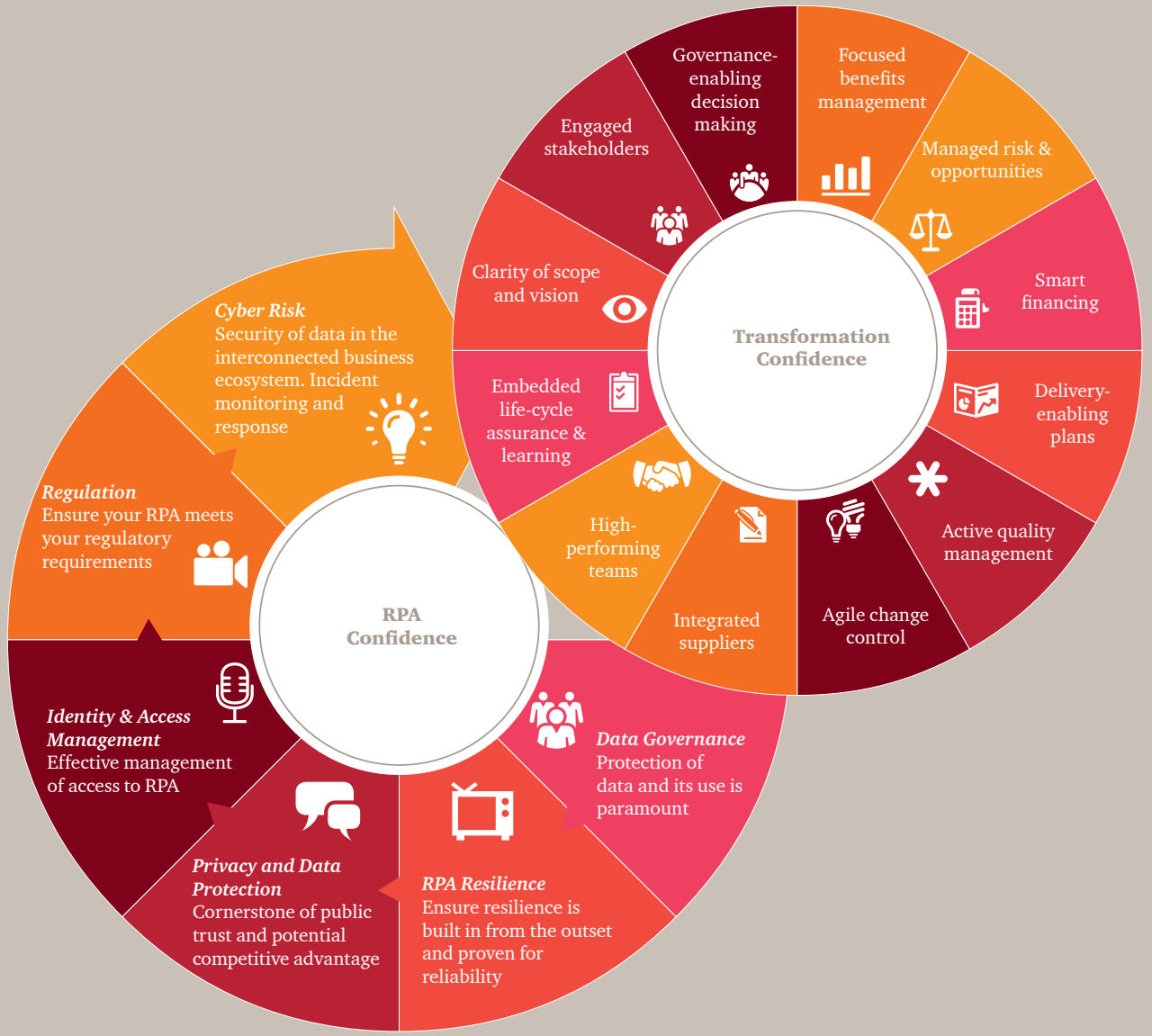
Within organisations there needs to be a shift from asking *How can we utilise RPA?* to *How does RPA impact our risk profile?* Early involvement of various corporate functions (such as compliance, risk and internal audit) is required to ensure a balanced discussion, risk assessment and agreement on the overall governance framework and process design.

Implemented correctly, the potential for RPA to reduce risk and improve compliance in business operations is clear. Consideration of these factors will help ensure that RPA is a friend.

Confidence in your RPA Transformation

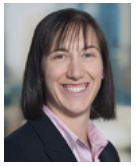
There is more to RPA than simply throwing robots at issues in operational processes.

To realise the benefits, RPA deployment must be managed with same discipline as any other project and the same consideration of the IT standards that need to be adopted. Our broader model of risk assurance is designed to give you confidence in both the health of the RPA implementation project and the controls in place that ensure benefits will be realised.



*Visit **pwc.com.au/rpa** regularly to read our latest thinking on Robotic Process Automation*

Find out more about Robotic Process Automation by contacting us:



Morven Fulton
+61 (3) 8603 3641
Morven.Fulton@pwc.com

Shane O'Sullivan
+61 (3) 8603 5333
shane.osullivan@pwc.com

Steven Rayment
+61 (2) 8266 1891
steven.rayment@pwc.com

Endnotes

1. See regulations 88 – requirements of assurance engagement, and 249 – Contents of assurance report.
2. MAS Technology Risk Management Guidelines, regulation 6.4.2 – 6.4.4, http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf.
3. https://www.pdpc.gov.sg/legislation-and-guidelines/overview.
4. https://www.pdpc.gov.sg/docs/default-source/advisory-guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(revised-8-may-2015).pdf?sfvrsn=2.

127037230