

RPA Program Playbook

Accelerating adoption of Robotic Process Automation (RPA) across the federal government through best practices, lessons learned, and proven strategies for RPA program development and maturity.

Version 1.1 - Published by the Federal RPA Community of Practice

January 17, 2020



LETTER FROM THE COP CHAIR

Federal Community,

We are proud to announce the initial publication of the Federal Robotic Process Automation (RPA) Program Playbook. This playbook is designed to provide federal agencies detailed, accessible guidance for initiating a new RPA program or rapidly evolving an existing program. We will periodically update this document to reflect developments in the federal RPA environment.

The RPA Program Playbook aligns closely with the President's Management Agenda's (PMA) aggressive cross-government goal to "Shift from Low to High Value Work" (CAP Goal 6). OMB is actively working, as part of CAP Goal 6, to rescind and modify requirements and regulations that increase agency workload. In addition to these burden reduction initiatives, another important element of CAP Goal 6 is workload elimination. All agencies are charged with pursuing workload elimination, and RPA provides a low-cost tool to make an immediate impact.

The opportunity for RPA to transform federal operations is massive. Current RPA programs operating within agencies are achieving roughly five hours of workload elimination per employee. If the government deployed RPA at scale and achieved only 20 hours of workload elimination per employee, the net capacity gained would be worth \$3 billion - and that is only scratching the surface.

Additional collaboration between agencies can help accelerate RPA adoption government-wide, as agencies are currently wrestling with common implementation challenges in a vacuum. In publishing this RPA Program Playbook, the Federal Community of Practice (CoP) will facilitate a government-wide conversation to overcome these common challenges. This includes sharing best practices and lessons learned from mature RPA programs, as well as resolving common technical, management, and operational issues.

I would like to thank the RPA champions at DHS, NSF, NASA, OPM, HUD, GSA, FRB, Treasury, OMB, and throughout DOD (Army, OUSD, OSD) for their strong contributions to this playbook. Contributors are included at the end of the playbook, allowing readers to identify RPA champions within their agency. Feel free to reach out to these leaders to start implementing this exciting technology immediately.

- Gerard

Gerard Badorrek
Federal RPA COP Chair and Executive Sponsor



Gerard Badorrek
GSA Chief Financial
Officer

TABLE OF CONTENTS

| Section Name | Page Number |
|--|-------------|
| Playbook Introduction | 4 |
| RPA Program Technology | 10 |
| Technology Infrastructure | 13 |
| Security Policy | 20 |
| Credentialing Policy | 26 |
| Privacy Policy | 29 |
| RPA Program Management | 31 |
| Operating Model | 35 |
| RPA Program Design | 40 |
| Management Reporting and Business Value | 48 |
| Process Selection, Assessment, and Improvement | 55 |
| HR Planning and Impacts | 63 |
| Operations Management | 65 |
| Appendix | 69 |

Note: The RPA Community of Practice developed this playbook with input from key federal RPA practitioners. This document should not be interpreted as official agency policy or mandated action.

Robotic Process Automation

Robotic Process Automation (RPA) is a low to no-code Commercial Off the Shelf (COTS) technology that can be used to automate repetitive, rules-based tasks. Like an Excel macro operating within a spreadsheet, RPA can record actions performed across a personal computer, access systems, and perform delineated tasks for human users. RPA products vary in their exact capabilities, but all RPA technologies emulate human actions, enabling process owners or staff with appropriate training to rapidly design, test, and deploy automations dramatically reducing an organization's low-value workload. Popular uses of RPA include data entry, data reconciliation, spreadsheet manipulation, systems integration, automated data reporting, analytics, and customer outreach and communications.

At a government-wide level, RPA can represent a profound change, with the potential to empower non-IT professionals and process owners with the tools to automate a significant share of their workload. RPA is considered transformative because it establishes the building blocks for artificial intelligence in terms of information technology infrastructure and task standardization. With effective RPA deployment, machine learning and intelligent automation are only a few, manageable steps away.

Many agencies across the federal government have initiated RPA programs to automate tasks of varying complexity. Automations developed to date have focused on multiple functional areas including finance, acquisition, IT, human resources, mission organizations, and security/mission assurance. Each RPA program, created to identify, build, and deploy automations has adopted different structures and approaches, ranging from closely-governed centralized programs to decentralized initiatives.

The benefits of RPA adoption within an agency can be significant. First, in alignment with the President's Management Agenda (PMA) Cross Agency Priority (CAP) Goal 6, RPA is an excellent tool for "Shifting from Low to High Value Work." Because RPA automates tasks, not jobs, it is primarily a tool for creating capacity and reducing organizational workload. This allows employees to focus on higher value-add work while their 'digital assistants' perform the standard/repetitive work.

RPA, however, is not just a workload reduction technology. It can be deployed to increase quality, reduce human error, increase compliance, strengthen controls environments, and to add new services to an organization's portfolio. For example, if an employee only has the bandwidth to audit a 10 percent sample of transactions, an RPA automation, running 24/7, may be able to audit the entire data set and send non-compliant records for adjudication.

From a government-wide perspective, the impact of wide-scale RPA adoption is massive. If agencies deployed RPA to save all civilian employees just 20 hours a year, that would equate to roughly \$3 billion in capacity created. Some RPA programs within the federal government have already achieved 5-6 hours of capacity per employee within their agency, indicating a modest and achievable goal. Within a few years of focused RPA deployment, the federal government could see substantial progress on many of the Administration's management goals in both terms of greater efficiency and greater ability to focus on high priority initiatives.

The Federal RPA Community of Practice

The Federal RPA Community of Practice (CoP) is a thought leadership and collaborative body designed to rapidly accelerate the adoption of RPA technology across the federal government. The CoP consists of representatives from more than 50 Federal agencies, with more than 750 members.

The RPA CoP pursues a bifurcated mission. First, the organization is charged with discussing and designing solutions to help individual agencies overcome the technical, management, and operational challenges that arise in deploying an effective RPA program. This portion of the mission includes important initiatives like designing common federal solutions for credentialing, privacy, and security, and designing common management metrics to gauge government-wide impact of RPA.

The second element of the RPA CoP mission is to provide knowledge sharing and mentoring to organizations looking to start an RPA program or to evolve their current RPA services. This RPA Playbook is a small part of the CoP's knowledge sharing efforts, which also include frequent cross-government collaborative meetings, communications, thought leadership pieces, webinars, and workshops.

The RPA CoP seeks to achieve its important mission with a sense of urgency and a bias towards action. As agencies continue to learn the potential benefits of RPA, enthusiasm for developing RPA programs government-wide grows exponentially. The RPA CoP plays an important role in helping agencies convert RPA enthusiasm into action. Specifically, the CoP helps agencies develop programs that are cost effective, auditable, avoid common pitfalls, and most importantly, deploy impactful automations.



RPA Program Playbook

This RPA Playbook gives federal agencies a detailed primer for initiating a new RPA program, as well as clear guidance for how to evolve existing RPA programs to achieve increased performance and maturity. Admittedly, this primer does not hold all of the answers for all of the challenges that arise on the RPA journey. To the extent answers can even be foreseen in advance, many of them will be agency-specific and not applicable across government. Instead, this RPA Playbook identifies the major decision points and steps along the journey and provides guidance based on best practices and lessons learned.

The key guidance and themes of the Playbook are summarized below:

1. **Just Get Started** - The CoP is definitely not recommending agencies jump into RPA without any planning. But once an organization has the proper initial planning in place, (goals, strategy, resourcing, RPA candidates, and executive buy-in) they should get started and launch the RPA program. Leadership must then operate with the understanding that active and agile management will be required to identify and mitigate ongoing challenges.
2. **Ensure Effective Collaboration Between the RPA Program and the CIO** - Agency CIOs play a critical role in creating a successful environment for RPA development, including the design of formal security protocols, credentialing, privacy processes, procurement of technology solutions, and enterprise governance. A close, working collaboration between RPA program leadership and representatives of the CIO can expedite RPA throughput.
3. **Establish Aggressive Goals and Deliver** - Similar to most new technologies, significant enthusiasm and excitement currently exists for the potential of RPA to transform federal agencies. It is important for RPA programs to quickly convert excitement into results, ensuring continued momentum and investment within agencies. Setting and communicating aggressive goals bolsters the ongoing business case for RPA - it is an inexpensive and low complexity solution for many operating challenges normally requiring expensive fixes such as system upgrades.
4. **Invest in Process Assessment and Improvement Capabilities** - With the addition of strong process assessment and improvement capabilities, RPA can transform business operations within an agency. Process improvement expertise is a catalyst for impactful RPA, as it helps an agency optimize RPA candidate selection and reengineer broad-scale business processes around the RPA application, increasing impact and value.
5. **Balance the Dual Priorities of Governance and Productivity** - Establishing a Center of Excellence or other management mechanism to centralize and standardize RPA governance is an important milestone for maturing an RPA program. However, RPA program and agency leadership need to carefully balance the benefits of governance, controls, and SOPs (whether IT or management) with ensuring high productivity and the deployment of impactful automations.
6. **Think Strategically about Technology Options** - Currently, well over a dozen proven RPA specific technologies, as well as, a host of enterprise systems with add-on RPA modules exist in the commercial marketplace. Given the complexity of the federal procurement process, it is important to invest time and energy up front to assess technology options. Agencies should focus on identifying a low-cost solution from a stable provider best aligned with their long-term program needs (e.g. functionality, cost, security requirements, technology capabilities).




INTRODUCTION - BENEFITS OF RPA

Why Deploy RPA at Your Agency?

Federal agencies are under continuous pressure to do more with fewer resources. Federal mandates require agencies to pursue operational improvements, greater efficiencies, increased capabilities, and technology modernization. Program managers must determine how to marshal diminishing resources to meet current workload and deliver on aggressive new federal and agency-specific requirements.

Robotic Process Automation (RPA) should be a prominent addition to a savvy program manager's toolkit.

- **Reduced Implementation Time:** RPA differs from traditional IT solutions in its ability to be rapidly designed and implemented. RPA automations are targeted solutions of limited scope and complexity. Because they mimic human interactions, costly business requirements analysis is not required. Moreover, because they are “low code” or “no code” solutions they require few technology resources. Program managers can **obtain significant results in a matter of a few weeks or months.**
- **Increased Organizational Capacity:** Because RPA automates tasks, not jobs, it is an effective means of creating additional capacity within your agency. Employees will be able to spend less time focusing on manual tasks, and more time on high-value work like data reporting, analytics, and operational improvement. Moreover, RPA is an inexpensive means to increase throughput and overarching outputs for critical business processes, allowing an organization to **do more for customers and partners.**
- **Improved Employee Engagement:** By automating manual, repetitive workload, organizations can achieve significant improvements in employee engagement. RPA automations increase employee quality of life by removing rote tasks, and enabling them to **focus on critical activities.**
- **Qualitative Benefits:** RPA deployments can achieve a host of qualitative benefits including: 1) increased accuracy; 2) increased compliance; 3) improved standardization and auditability; 4) lower response times and increased customer satisfaction; 5) reduced process cycle times; and 6) increased measurability and transparency.
- **Applicability of RPA Across Functions and Agency Priorities:** An investment in RPA technology can have almost universal applicability across your organization. See the chart below for a brief description on where RPA can be leveraged within your agency.

| INTERNAL OPERATIONS | TECHNOLOGY ENHANCEMENT | ACCOUNTABILITY AND AUDIT | DATA ANALYTICS AND REPORTING |
|---|---|--|--|
|  |  |  |  |
| Common Use Cases <ul style="list-style-type: none">• Finance• Human Resources• IT Services• Procurement• Administrative Services | Common Use Cases <ul style="list-style-type: none">• Systems Integration• Enhanced System Functionality (add-ons).• Data Verification and Validation | Common Use Cases <ul style="list-style-type: none">• SOP Compliance• Transaction Reviews• Automated Controls• CAP Management• Risk Assessment and Surveying | Common Use Cases <ul style="list-style-type: none">• Automated Data Reporting• Data Gathering and Cleansing• Data Mining• Performance Monitoring |

INTRODUCTION - COP MISSION

Accelerating Government-Wide Adoption of RPA

Federal agencies are currently at multiple points in the RPA journey. A recent survey conducted by the Federal RPA CoP suggests there are roughly 25 organizations in the federal government that are piloting RPA technology or have a few automations in production. Approximately 10 more programs have 5 or more automations in production, and a further 5 programs have 20+ RPA automations deployed.

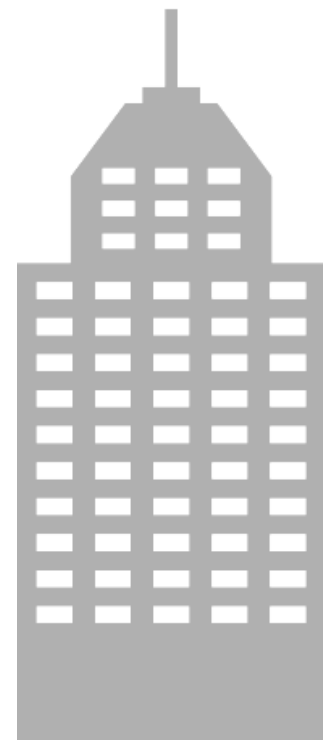
In designing this Playbook, the COP sought to provide support and guidance to all federal RPA partners — from those considering RPA, to those who have robust programs in place.

The maturity model below represents the CoP's thinking on how best to gauge the evolution of RPA programs and the types of indicators/milestones needed to convey agency progress in improving and growing RPA capabilities.

The chapters in this playbook are dedicated to presenting best practices, lessons learned, and advice for how every federal RPA program can climb the maturity ladder. Within these chapters, 10 capability areas are discussed in significant detail, providing readers with an understanding of how progress within these areas will lead to broader agency success in increasing RPA program maturity and value.

RPA PROGRAM MATURITY MODEL

| Start-Up RPA Program | Emerging RPA Program | Impactful RPA Program | High-Performing RPA Program |
|--|---|--|--|
| LEVEL 1 <ul style="list-style-type: none">• Pilot bots underway or <5 bots in production.• Less than 5k hours of annualized capacity created.• Establishing formal processes related to RPA. | LEVEL 2 <ul style="list-style-type: none">• 5-20 bots in production,• 5-50k hours of annualized capacity created.• Initial security, privacy, and ATO policies formally defined.• Developing program management, reporting, and process improvement capabilities. | LEVEL 3 <ul style="list-style-type: none">• 20+ bots in production.• 50-100k hours of annualized capacity created.• Formal ATO, IT Security and Privacy policies.• Strong program and operations management.• Strong process improvement capabilities.• RPA solutions implemented across multiple functional areas.• Robust pipeline of future opportunities. | LEVEL 4 <ul style="list-style-type: none">• 5-10 bots deployed monthly.• 100k+ hours of annualized capacity created.• COE Model—bots generated from multiple business units.• Intelligent automation capabilities.• Dedicated (FTE) program management, process reengineering, and development capabilities.• Workforce redeployment, capacity planning, and reskilling required.• Enterprise platform for unattended bots. |



INTRODUCTION - RPA PLAYBOOK CAPABILITY AREAS

RPA Capability Areas

The matrices below depict the 10 RPA capability areas an agency would need to address to progress along the RPA program maturity model. For ease of reading, the capability area descriptions are truncated with full descriptions contained in each of the dedicated sections in the playbook.

It is important to note the CoP is not recommending every agency progress from Level 1 to Level 4, sequentially, in all areas. For compelling business reasons, agencies may choose to skip Level 1 or Level 2 in some areas, particularly if the program intends to act as agency-wide RPA provider.

RPA Technology

| Capability Area | Description | Maturity Model | | | |
|----------------------------------|---|----------------|----|----|----|
| | | L1 | L2 | L3 | L4 |
| Technology Infrastructure | Selecting, building, operating, and maintaining a secure and scalable IT platform for development, testing, and production. | | | | |
| Security/ATO | Designing streamlined Security/ATO processes to ensure safe and rapid deployment of automations. | | | | |
| Credentialing | Designing compliant credentialing processes aligning with RPA program resourcing and technology strategies. | | | | |
| Privacy | Developing processes to meet relevant federal privacy and ethics standards for the deployment of RPA. | | | | |

RPA Program Management

| Capability Area | Description | Maturity Model | | | |
|--|--|----------------|----|----|----|
| | | L1 | L2 | L3 | L4 |
| Operating Model | Establishing an effective oversight and management framework to foster cross-agency collaboration and accountability. | | | | |
| RPA Program Design | Designing an RPA program structure to meet established throughput goals and deployment strategy. | | | | |
| Management Reporting and Business Value | Creating program-specific and government-wide RPA implementation and operations metrics, strategies, and business case models to drive common measurement and impact analysis. | | | | |
| HR Impacts | Drafting HR processes and guidance to address the impacts of RPA including employee reskilling, redeployment, and satisfaction. | | | | |
| Process Assessment and Improvement | Identifying and assessing processes for automation that maximize the value of RPA within an agency. Leveraging RPA effectively as a tool for broad process improvement within an agency. | | | | |
| Operations Management | Defining processes for developing automations, scheduling automations, facilitating capacity management, license management, and monitoring/fixing errors. | | | | |

SECTION 1

RPA Program Technology

1. Technology Infrastructure

2. Technology Policy

- Security
- Credentialing
- Privacy



RPA MYTHBUSTERS - TECHNOLOGY EDITION

Dispelling a few myths and misconceptions about RPA in the federal government ...

1

There is one technology infrastructure strategy that all agencies should follow.



The technology infrastructure strategy used for evolving from RPA pilot to high-impact program should be agency-specific and incorporate agency business strategy, RPA goals, resourcing levels, existing agency technology strategy, operational realities and structures, and program requirements (demand).

2

No guidance exists for credentialing non-humans.



No authoritative guidance exists for credentialing non-humans specific to RPA, but existing OMB, FISMA, and NIST directives speak to this issue from an automation technology perspective. Multiple agencies have adapted these sources to develop robust, safe, credentialing strategies for non-humans within the RPA context.

3

Every RPA automation project requires a new Authority to Operate (ATO).



The common security approval strategy is for the overarching RPA software or technology to receive a formal approval from the agency's CIO/CISO and each automation project created using that software to complete a limited, lower-level, approval specific to its functionality.

4

RPA will soon be out of date. Let's just wait for AI.



RPA is an important stepping stone to AI because it establishes the right technology structures, technology competencies, organizational culture, and standardized business processes to adapt AI. Transitioning from manual, repetitive, workload straight to machine learning or other advanced AI tools is often a leap too far. RPA sets agencies on an effective path.

5

RPA should never touch PII. It's too risky.



Many agencies across the federal government are currently running RPA automations that manipulate and store data containing PII. While this functionality does require an additional set of approvals, getting them is not an insurmountable task, and most agency privacy officers already have clear procedures in place for getting approvals to access and manipulate PII.

MATURITY MODEL ALIGNMENT

| Start-Up RPA Programs | Emerging RPA Programs | Impactful RPA Programs |
|--|---|---|
| LEVEL 1 <ul style="list-style-type: none"> Initial technology selection Desktop model | LEVEL 2 <ul style="list-style-type: none"> Enterprise software selection Virtual desktop model | LEVEL 3 <ul style="list-style-type: none"> Enterprise software deployment and infrastructure Enterprise platform model |

Level 1: Technology Infrastructure for Start-Up RPA Programs

Technology Selection for Start-Up RPA Programs

To select the most appropriate technology for an RPA pilot, start with a firm understanding of initial proposed automation opportunities. As detailed in the Process Selection section of this playbook, the pilot automations should be low complexity - meaning they should only interact with a few systems, with consolidated ownership and relatively few stakeholders.

A full review of technical requirements for the future RPA program is not required at the pilot stage. However, the CoP does recommend RPA program staff assess the requirements of the pilot opportunity against vendor capabilities including cost factors, ease of use, technical criteria, and availability of vendor support.

The program should also determine which vendor solutions may already be on the agency's Technical Reference Model (TRM) or Software Product Listing (SPL) of approved technologies. Solutions already approved to run on an agency's network(s) can be deployed with expedited procurement and approvals processes. Most agencies also offer a waiver process for pilot programs outside the SPL or TRM List.

Agency CIOs or technology management offices should be consulted throughout the selection process for the RPA pilot technology. These groups likely already have a formal process in place for evaluating potential vendors, existing contracts to expedite acquisitions, and the knowledge and infrastructure to help a start-up RPA program make a smart choice in selecting pilot technology.

Pilot Technology Evaluation Factors:

- 1. Technical Criteria** - includes agency-specific operating system and hardware requirements, as well as the technical capabilities needed to fully deploy the selected automation.
- 2. Cost** - includes initial setup costs, licensing costs, and maintenance costs for the pilot automation. Vendors can offer price incentives for testing and piloting technology.
- 3. Ease of Use** - includes the ease of coding/automation development and ease of interacting with systems relevant to the specific automation opportunity.
- 4. Vendor Support** - most vendors offer ongoing support, training, and customer outreach to assist agencies in completing pilot bots. This would be less critical if an agency were using contractor support to build the automation.

Desktop Model

Deploying attended automations using a “Desktop Model,” is the quickest path for a start-up RPA program to develop proof of concept. In the Desktop Model, the RPA solution leverages the processing power of one workstation and one user’s credentials.

When this model is used for a pilot project or proof of concept, the user generally starts the automation employing his or her credentials to access enterprise networks and multiple systems on the desktop to gather data and run the automation.

In launching and designing the pilot program, it is recommended to work with the CIO shop for approval to download and access RPA software.

Although this platform does not require significant upfront investment in IT infrastructure (cloud or on-premise), it is limited in capability because of challenges in scaling automations to larger user populations. Deploying attended automations run by process custodians must integrate separation-of-duty controls that prevent the custodian from being able to alter automation coding.

As an RPA program matures its technology infrastructure, these automations can easily be retrofitted and deployed live using either the Virtual Desktop Infrastructure (VDI) or enterprise platform that provides oversight and tracking of automations.

In sum, the Desktop Model is recommended for a pilot project because it gives the RPA program an opportunity to gauge the technical feasibility of the vendor solution, plan future operational costs, and measure technical capabilities against future requirements. Program leaders might also consider a related alternative to the desktop model - RPA as a Service (RPAaaS). These offerings from several leading vendors and service providers offer the speed and ease of the desktop approach while reducing security concerns because no software is installed locally. One potential issue of RPAaaS to consider is on-network data and resources may not be accessible from the public cloud services, so pilots may be limited to automations involving public data sources.

Approach #1 - Desktop Model

Description: The Desktop Model is best suited to running a pilot project or proof of concept. While technically less complex than other RPA infrastructure approaches, it lacks the scalability, functionality and controls to support a large RPA program.

| | | | |
|--------------|--|--------------|---|
| Pros: | <ul style="list-style-type: none"> • Low Investment • Rapid Implementation • Low Financial Risk • Low Technical Complexity | Cons: | <ul style="list-style-type: none"> • Limited to Attended Bots • Limited Scalability • Audit/Security Risks |
|--------------|--|--------------|---|

Security Implications Security and audit concerns - difficult to enforce standardization, controls, or policies with desktop software running on individual laptops.

Credentialing Implications Low complexity - automations run using existing human credentials and user access to systems.

Privacy Implications Privacy concerns - data types and systems accessed through the desktop model raise privacy concerns and would keep the automation from ever going “live.”

Level 2: Technology Infrastructure for Emerging RPA Programs

Enterprise Technology Selection for Emerging RPA Programs

There are currently numerous RPA technologies on the market, in addition to multiple Business Process Management (BPM) solutions with dedicated RPA modules. Deciding which of these solutions will best serve an agency’s RPA program can be daunting.

TECHNOLOGY INFRASTRUCTURE

But if an RPA program has a clear long-term strategy and defined technical requirements, the assessment and selection can be completed in as little as 6-8 weeks while work continues towards a pilot. In addition to reviewing technical capabilities, it is important to conduct vendor demonstrations that address primary use cases, and speak with references to ensure strong alignment with the preferred supplier.

Agency CIOs have the expertise to help RPA programs align requirements with capabilities and should be able to help create a finite list of options for leadership. Agency enterprise architects can determine the best strategy for selecting an RPA technology that fits into the overarching IT environment.

The figure below provides a sample set of criteria to consider in making an enterprise technology selection. The agency CIO will likely have an existing process, as well as expertise and acquisition vehicles to assist the RPA program in identifying and procuring the optimal technology package.

Factor 1: Vendor Experience



- Market Presence
- Commercial Experience
- Public Sector Experience
- Industry Recognition
- Customer References
- Contracting Considerations

Factor 2: Product Features - Process



- Workflow Management
- Process Recorder
- Self-Learning Capabilities
- Ease of Use
- Process Assessment Functionalities

Factor 3: Product Features - Automation



- Visual Authoring Tool
- Command Library
- Attended/Unattended Automation Capabilities
- Component Sharing
- Test/Debugging Controls
- Ease of Use

Factor 4: Security



- Application Security
- Credential Management
- FedRAMP Compliance
- ATO Experience
- Risk/Security Assessments
- Certifications
- Data Encryption/Protection
- Process Traceability

Factor 5: Product Features - Operations



- Centralized Bot Deployment, Management, and Scheduling
- Licensing Structure
- Volume, Scalability, and Workload Management
- Exemption/Exception Handling
- Dashboard Capability
- Business Analytics
- Operational Analytics

Factor 6: Architecture



- Hardware/Software Requirements and Virtualized Servers
- Multi-Tenant Support
- On Premises (Desktop/Server)
- Cloud (Public/Private/ Hybrid)
- Availability and Disaster Recovery Capabilities
- Network Bandwidth Impacts

Virtual Desktop Model

Several leading agencies used a VDI to accelerate RPA adoption, complete pilot automations, and even deploy automations at scale. VDI can serve as a bridge between individual desktop piloting and full enterprise solutions. In order to get started with the VDI model, it is recommended to work in conjunction with the CIO shop to determine the suitability of using a VDI environment for the agency's RPA solutions.

A VDI environment centrally-managed by IT has some of the benefits of an enterprise model with little initial investment if the agency already has VDI capability. In a VDI, computing resources can be quickly and easily provisioned without physically acquiring new infrastructure.

This model is more robust and secure than the desktop model as separate environments are created for development, test and production, and role-based access control (RBAC) can be used to restrict user access. Another key control is that the software maintenance and upgrades are managed centrally, and servers can be easily rebuilt and reconfigured as needed. Because of segmented environments, VDIs provide higher availability than an individual desktop and automated backups can aid disaster recovery. Before implementing this platform, the RPA project team must evaluate RPA software tool compatibility with its own organization's VDI setup.

Using a VDI environment to start allows the organization to place automations in production while gaining experience and knowledge in many aspects of RPA. This also allows organizations to continue to automate processes while the agency is ensuring funding, building, testing and getting an ATO for an enterprise platform. The experiences to be gained during this period will include opportunity identification and assessment, documentation, development, security and privacy approval process definition, and operations management. Agencies can begin achieving the benefits of RPA many months earlier and gain valuable experience in implementation and operations while the enterprise platform build is underway.

While VDIs were traditionally operated in an organization's on-premise data center, it is more common for VDIs to be provisioned in virtual private cloud (VPC) environments. As an alternative, the VDI model could be deployed in a public cloud environment, providing many of the advantages of added governance to organizations without virtualization technology in place.

Approach #2 - Virtual Desktop

Description: Virtualization offers organizations more control and security over desktop installations as they mature toward an enterprise-grade solution. It enables a small team to start building the policies and procedures necessary to grow an RPA program beyond initial test bots.

| | | | |
|--------------|--|--------------|--|
| Pros: | <ul style="list-style-type: none"> • Limited Investment • Attended or Unattended Automations • Small Team Integration | Cons: | <ul style="list-style-type: none"> • Requires Existing VDI Environment • Difficult to Scale • Limited Security provisions • Third Party Tool Integration |
|--------------|--|--------------|--|

Security Implications More centralized management enhances overall security posture.

Credentialing Implications User or bot credentials with proper authority required to access target systems.

Privacy Implications Limited RBAC provides some data protection via user segmentation.

Level 3: Technology Infrastructure for Impactful RPA Programs

Enterprise Technology Implementation for Impactful RPA Programs

The transition to an enterprise RPA technology solution is a significant investment and a complex undertaking. While the RPA software will likely remain unchanged unless major capability gaps are identified, the implementation of the solution requires a detailed architecture plan to ensure the platform can function as an enterprise service. This shifts applications from often single node instances to distributed services where data, messaging, compute and security layers are segregated and housed on specialized infrastructure. In addition, infrastructure replication has to be considered in order to satisfy high availability and disaster recovery requirements as well as to balance usage loads.

Enterprise Platform Model

The Enterprise Platform model is the ultimate destination for hosting and running automations—unattended, attended and hybrid bots. This platform provides the ability for an RPA program to operate at scale, and requires enterprise-wide deployments where security, workflow and governance are critical to long-term success. The enterprise platform provides an agency with the ability to monitor and manage automations in a centralized way while integrating with enterprise-grade IT solutions and infrastructure that are already in place, (e.g., email and identity management).

To maximize the benefits of RPA, organizations must operate the technology as a mission-critical enterprise service. Key characteristics of enterprise systems include:

- **Available 24/7/365:** The Enterprise Model provides predictable and dependable continuity of service, and can be designed to include high availability and disaster recovery (HADR). The platform also allows for real-time processing of scheduled automations.

- **Speed and Accuracy:** The Enterprise Model allows for a reduced process cycle-time through flexible compute resourcing delivering a reduced risk of transactional errors for an improved customer experience.

Approach #3 - Enterprise Platform

Description: Software and IT infrastructure system designed to support mission-critical services. They are generally complex, scalable, component-based, and distributed, offering high availability/disaster recovery.

| | | | |
|--------------|---|--------------|--|
| Pros: | <ul style="list-style-type: none"> • Fully scalable resource • Security Compliance for Government agencies • Program-level Management • Centralized Deployment and Scheduling | Cons: | <ul style="list-style-type: none"> • Cost/License Fees • Lengthy Implementation time • Enhanced Team Skills Required to Operationalize • Full ATO Required |
|--------------|---|--------------|--|

Security Implications Robust FIPs compliant (140-2) encryption protects data at rest and in transit; authentication via Active Directory or SSO.

Credentiaing Implications Secure password vaults and integration with third party credential managers.

Privacy Implications Granular role-based access control (RBAC) across all functions and GDPR compliance support address data privacy.

Enterprise Platform Model

- **Consistency and Scalability:** The enterprise model ensures a more stable environment through centralized management while allowing a program to scale in the running of automations.

An enterprise platform enables an organization to operate an RPA program with the transparency and security required for mission-critical applications. It provides the capability to oversee every automation from one centralized service that is able to schedule, monitor, and manage all automations. The life-cycle of automations from design and development to testing and deployment is managed using enterprise infrastructure already in place. The platform also operates with enterprise-grade security protocols and frameworks and full auditability of every automation is provided allowing administrators a comprehensive view of automation activities.

As RPA programs mature, the tendency is for stakeholders to expect the technology to solve more complex use cases. This often involves the integration of complementary technologies to RPA, including process mining, business process management, machine learning, and other intelligent automation applications. An enterprise platform provides a flexible architecture to plug-in additional services to the overall solution to address these more challenging automations.

A final benefit of the enterprise environment is typically a full suite of analytical tools to help organizations measure program performance. Dashboards are available at both the operational level to assess automation activities, such as utilization, error rates, and runtimes, as well as at the strategic level to offer leadership insights on program impact, such as return on investment and efficiency metrics.

Note: The planning and strategy development for a well-designed RPA technical infrastructure would benefit from a review of common industry technology management approaches and concepts like IT Infrastructure Library (ITIL) or Capability Maturity Model Integration (CMMI).

TECHNOLOGY POLICY - CONCEPT SUMMARY

Agencies must work closely with the CISO, CIO, CPO, and other technology leaders to obtain approvals for the adoption of RPA technology. This playbook shares current approaches to these technology policy issues, as well as key decision points that other federal agencies have encountered.




AREA 1: Security

Security - RPA programs need authority to operate (ATO) select applications and enterprise platforms/services within an agency's IT environment. This usually requires a formal decision by an approving body within an individual agency's CISO, CIO, or technology management office.

Security and software approval processes vary by agency (including between civilian and defense), but generally require a review of the selected IT solution, an understanding of how the RPA program intends to deploy the solution, identification of any security risks, and an assessment of relevant agency and federal standards, policies, and requirements.

Once an initial software approval for the RPA platform is granted, there may be ongoing requirements. For example, future automations may need approvals from the CIO or CISO, including documentation, questionnaires, and/or impact assessments. Close collaboration with the CIO and CISO organizations is required to expedite software approval processing or it can become a significant hurdle for a new or developing RPA program.



AREA 2: Credentialing

Credentialing - Federal and agency-specific credentialing policies are promulgated to manage RPA identity and access to IT systems and data. These policies establish a formal process for authenticating users, monitoring access rights and ensuring relevant security policies are upheld. In the context of Robotic Process Automation, credentialing is critical: RPA automations access systems and data in the same way humans do.

RPA programs must collaborate with their CIO or technology management office on how the agency will recognize and authenticate digital workers (RPA automations) with non-person entity credentials (NPEs). To date, these approaches generally mirrored the same processes used for credentialing human workers, with each automation granted an identity depending on existing agency policy. In some cases, agencies have allowed attended RPA automations to inherit the credentials of their human operators.

Regarding ongoing requirements, RPA programs must monitor access rights and credentials to ensure continued compliance. For each automation, RPA programs must assess credentialing and privacy issues make sure the automation has the permission levels required to interact with all necessary systems.



AREA 3: Privacy

Privacy - While Security/ATO and Credentialing are policy challenges largely addressed at the program or enterprise-level, privacy concerns around RPA are specific to individual automations. All agencies have privacy policies in place to govern how data is stored, accessed, and used. The applicability of those privacy policies will be specific to the capabilities and functionality of individual automations designed by the RPA Program.

In general, privacy thresholds for RPA depend on the sensitivity of the data processed by the automation. The RPA program should work with the CPO, Senior Agency Official for Privacy, CIO or technology management shop to design clear policies for interacting with data at each relevant sensitivity level. For automations that handle Personally Identifiable Information (PII), formal Privacy Threshold Assessments (PTA) may be required to identify potential risks and ensure adequate safeguards. For less sensitive data, a Privacy Threshold Assessment (PTA) could be populated with approvals by the Senior Agency Official for Privacy (SAOP).

MATURITY MODEL ALIGNMENT

| Start-Up RPA Programs | Emerging RPA Programs | Impactful RPA Programs |
|---|---|--|
| <p>LEVEL 1</p> <ul style="list-style-type: none"> Identify security and risk considerations Involve CIO, risk, and compliance groups | <p>LEVEL 2</p> <ul style="list-style-type: none"> Implement repeatable processes for approvals and ATO Deploy to secure VDI infrastructure | <p>LEVEL 3</p> <ul style="list-style-type: none"> Integrate RPA into IT security and governance Integrate RPA into ISCM |

Level 1: Security Policy for Start-Up RPA Programs

RPA programs must work in close collaboration with the CIO or the technology management office to obtain the proper security and access approvals for their selected RPA technology. With no targeted guidance or policy available on security approvals for RPA platforms nor individual automations, this process must adhere to relevant existing federal and agency-specific requirements. This section lays out the common decision points and challenges for RPA programs seeking security approvals, enabling start-up RPA programs to begin informed discussions with their CIO.

An RPA implementation creates a software application that processes, transmits and stores an agency's data. The Federal Information Systems Modernization Act of 2014 (FISMA) requires a federal agency to assess and manage the security and privacy risk to the confidentiality, integrity, and availability of that data using a formal program compliant with Federal Information Processing Standard (FIPS) 199. These requirements must be met using a structured NIST-based framework to support consistent, informed, and ongoing authorization decisions.

The start-up program is where an agency begins building foundational security needs into the planning and development of the RPA software, and in this context there are three focus areas: 1) security of the platform itself; 2) Access management for individual automations; and 3) security of data affected by the automation.

What types of security approvals are required for RPA platforms?

NIST guidance requires the creation of a System Security Plan (SSP), including comprehensive documentation of a system, its sub-systems, components, and processes. The SSP includes the FIPS 199 Security Categorization, which determines the security risk impact rating and the baseline of controls that must include the controls needed for the security of the RPA technology to be authorized in the system. RPA approval documentation and control evidence may be included in a system's sub-system or system component supporting documentation. Approvals needed for an RPA program or project vary by agency but are also dependent upon the size, scope, and the risk presented by the RPA implementation.

SECURITY POLICY

What factors should influence the security approval process for individual automations?

The risk introduced by the RPA implementation.

- The original information system categorization risk rating (low, moderate, or high).
- Whether the RPA implementation introduces unique risks raising the high-water mark (e.g., modifications to PII, cryptography, protocols, services, and/or ports).
- The credentialing strategy - whether RPA is using User IDs or NPE (including whether automations are attended or unattended).
- The type of automation authentication (e.g., single sign-on, multi-factor authentication, smart card, PKI, LDAP, Kerberos, SAML, Open ID).

The scope of the RPA implementation.

- The functionality of the RPA automation - what is it designed to do? (e.g., an automation responsible for moving data between two financial systems will require a greater deal of scrutiny than an automation responsible for providing status notifications).
- The number and type of systems the automation interfaces with, including whether any of the systems have special security designations or accreditations.
- Audit, process, and performance risks associated with the automation deployment.
- RPA program design elements including whether a custodian manually runs the automation, whether formal controls are in place and monitored, and the type of technology deployment (desktop, VDI, or enterprise platform).
- The automation's operating environment (development, test, or production).

The scope of the RPA authorization.

- Whether the automation processes, transmits, or stores data within single or multiple authorization boundaries.
- Whether the automation processes, transmits, or stores data at more than one agency.
- Whether the automation processes, transmits, or stores data using cloud or shared service providers (external to the agency).

What groups within an agency should be involved in the security approval process?

Depending upon an agency's internal management policies, the stakeholders involved in the security approval process might have different roles and responsibilities. The RPA Program is an important integrator for all relevant stakeholders to ensure a consistent security approval process is designed, deployed, and communicated.

- CIO - Concerned with IT strategy and alignment with business objectives, and ensuring IT infrastructure, design, and development platforms can support business objectives securely in a cost effective manner.
- CISO – Concerned with the security and privacy of business information and compliance with all federal laws, regulations and statutes. Manages risk to the confidentiality, integrity, and availability of information processed, transmitted, and stored by agency information systems.

SECURITY POLICY

- Chief Privacy Officer – Concerned with protection of personally identifiable information of employees, contractors and members of the public processed, transmitted, or stored by agency information systems.
- Information System Owners – Concerned with preparation of the authorization package for the authorizing official, including the SSP, risk management, and monitoring of relevant systems.
- RPA Program - Concerned with integrating the RPA program into the agency's information technology infrastructure and security architecture and working with the agency's CIO or technology management office to develop a security approval process meeting security and privacy requirements, while not creating an undue burden for automation deployments.

How can Start-Up RPA Programs get security approvals?

In the initial phases of an RPA program, approval will be needed to use RPA software that allows development and testing on a desktop. The RPA CoP recommends an initial consultation with the CIO or technology management office to confirm whether and how trial software or limited licenses can be procured to begin piloting RPA.

For a pilot or proof of concept project, an authorizing official may use an authorization decision limited by time and scope, as defined in NIST Guideline SP 800-37 Revision 2. Those options could include an authority to proceed, authority to use, interim authority to operate, or interim authority to test.

An authorization package must identify, address, and document the unique risks associated with the RPA software. In consultation with the CIO or technology management office, the RPA program will need to collaboratively develop RPA-specific policies, procedures, and guidelines that satisfy control, approval, and risk mitigation requirements. These can include elements such as:

- ISSO or IT security representative designation letter
- Security specification documents and clear IT security approval requirements
- Security Requirements Traceability Matrix (SRTM)
- Separation of Duty Matrix (SoD)
- Security and privacy questionnaires, checklists, and security configuration baseline
- Access request and approval forms
- Privacy Threshold Analysis (PTA)
- Formal software development and gating process
- Code walkthroughs, peer reviews, and ADMIN testing
- Security impact testing and validation
- Formal rules of behavior
- Issue logs and risk watch lists

Creating such evidence in a cost-effective and efficient manner is important, especially for start-up and pilot RPA projects and programs.

Level 2: Security Policy for Emerging RPA Programs

Security Considerations Unique to the Virtual Desktop Infrastructure (VDI)

The virtual desktop model requires the use of virtual server technology to run the selected RPA software. The two main advantages of a VDI environment are: 1) the ability to separate the development, production, and test environments which strengthens controls; and 2) the ability for custodians to run attended automations without losing the use of their own personal desktops (minimizing down times). These are additional capabilities over the desktop model (Level 1), and it greatly decreases the security risks associated with developing, testing, and deploying RPA automations. Specifically, the use of VDI supports the use of repeatable security, privacy, and credentialing processes for an RPA program and the segregation of clearly defined roles and responsibilities. Together, these standardized processes and roles constitute a “standard configuration” for RPA implementation and align with Software Development Lifecycle (SDLC) best practices.

The Community of Practice has identified security policy considerations unique to the VDI model:

- **Segregation of environments:** Separate environments should be designated for development, testing, and production environments. The developer should have access to the development and testing environments, but not the production environment. Access to each of these environments should be granted through a secure portal and an IT ticket request process. The automation software should be loaded into the virtual environment by IT staff.
- **Segregation of duties:** aligned with the segregation of environments, the segregation of duties associated with the VDI environment bolsters security ensures the same people who code the automations are not also responsible for their daily (or weekly) operations.
- **Assignment of automation custodians:** In the Virtual Desktop Environment, automation custodians should be designated to run attended automations. These individuals understand the process of the automation and should receive access to the production environment using authorized agency identity and access management services.
- **Control of code:** During this maturity phase, the RPA program should begin developing centralized storage and management of reusable code. Controls will need to be developed and implemented to ensure code can be saved without alteration by other program developers.

Obtaining Individual Automation Approval (Depending on Agency Policy)

In order to comply with federal security mandates, in the Virtual Desktop Environment, agency security teams might require individual automation approval before an automation is allowed to be deployed into the production environment. Individual approval for automations could encompass any number of the following pieces as decided by an agency's CIO office:

- **Process Design Documentation (PDD)** - As part of the individual automation authorization package, the security team will most likely require each project to have its own process design document. The PDD is a detailed document that first lays out, in detail, the overall aim of the automation project. It requires a detailed definition of what is to be automated while also incorporating a current state and future state process diagram. This document will also include keystroke level documentation of the automation project while detailing each system involved in the automation. This document acts as the 'contract' between the process owner and the RPA project management office on what will be automated.
- **FISMA Security Questionnaire** - All federal agencies need to manage the risk to the confidentiality, integrity, and availability of the data and systems affected by an deployed RPA solution.

SECURITY POLICY

To comply with FISMA and FIPS, some agencies develop a detailed but business-user friendly security questionnaire to gather information to complete the SSP. The questionnaire gathers information about testing and development processes, expected lifetime of the RPA project, user accounts and groups, levels of access needed (read, write, user admin, etc.), interconnections, and whether or not the program stores encrypted data stored or in transmission.

- **Privacy Threshold Assessment (PTA)** - A Privacy Threshold Assessment is a questionnaire used to determine if a system contains personally identifiable information (PII), whether a privacy impact assessment is required, and if any other privacy requirements apply to the automation. A PTA should be completed when developing a new automation as the automation can collect, store, or process identifiable information. A PTA will determine if a PIA is required.
- **Privacy Impact Assessment (PIA)** - A Privacy Impact Assessment might be required if the automation is handling PII. A PIA is an analysis of how information in identifiable form is collected, maintained, stored, and disseminated, in addition to examining and evaluating the privacy risks and the protections and processes for handling information to mitigate those privacy risks.
- **System Owner Approval** - Individual system owner approval may be required as part of the overall approval package for each automation. Some agencies may have instituted formal procedures and a standard template for RPA automation, requiring approvals from the process owner, system owner, and the ISSO. If data is transmitted between agency systems, a Data Sharing Agreement (DSA) may be required. If data is transmitted between agencies, or third parties, an Interconnection Security Agreement will be required, and a Memorandum of Understanding or Agreement (MOU/MOA) may be needed.
- **Video Demonstration of Automation** - A video demonstration of a developed automation may be required. This step-by-step video should include a walkthrough of the automation with voiceover to discuss how the automation is running and detailing each step in the process. This will give agency stakeholders (CPO, CISO/CIO) an understanding of how the automation will operate within its environment, which can expedite the approval process.
- **Custodian Rules of Behavior (ROB)** - A Custodian Rules of Behavior document may be required as part of the authorization package for attended automations in a Virtual Desktop Environment. An individual, separate from the process owner or developer and typically from within the business unit of an impending deployed automation, must be authorized to run specific automation. This must be done in a formalized and documented way with the custodian acknowledging the rules of running an automation.

Level 3: Security Policy for Impactful RPA Programs

Security Considerations Unique to the Enterprise Environment

As an agency's RPA program matures and scales, it will need to integrate into the agency's enterprise environment to help manage the automations that have been developed. The benefits of the enterprise environment include the ability to schedule the automations, the ability to track and look at real-time analytics on the productivity of the deployed automations, and to centrally manage the deployment of each automation. This platform allows for a clear segregation of environments between a development, test, and production environment while allowing for a systems administrator to manage the enterprise platform.

SECURITY POLICY

The Community of Practice identified a few security policy considerations unique to the enterprise platform environment:

- **Account Management** - Authentication and granting of privileges (account authorization) of RPA accounts is closely tied to credentialing . More detail can be found in the Credentialing practice area section. Enterprise security programs define access and account management through Identity and Access Management (IAM) policy, procedures, tools, and security controls used in an agency's security architecture. What is required, or prohibited depends upon the purpose, function, and enterprise environment and can range widely, but include SSO, MFA, Smartcards/PIV, PKI, biometric, tokens, CASB, etc.
- **Audit Logging**—Every transaction executed by an RPA process is recorded to provide a full audit trail. Ideally, in an level 3 enterprise, audit logs are managed centrally by a Security Incident and Event Management (SIEM) system that monitors and alerts staff of abnormal activity. Some vendors offer orchestration solutions that implement some of the features of Security Orchestration Automation and Response (SOAR) systems.
- **Configuration Change Management** - All changes in the enterprise development, test, and production environments are usually documented fully and maintained for audit and rollback purposes. At the enterprise level, changes to all configuration control items are automated, as are many security controls, and moving programs from test to the production environment. The effectiveness of change control, security controls and tools, patch and release management must be tested and audited regularly.
- **Data Transmission** - RPA automations may transmit data across authorization boundaries, or even agencies. In that case, additional documentation, such as Data Sharing Agreements (DSA), Memoranda of Understanding or Agreement (MOU/MOA), or Interconnection Security Agreements (ISA) will be required. Best practices dictate data be encrypted using FIPS140-2/3.
- **Information Security Continuous Monitoring (ISCM)** - The Department of Homeland Security (DHS) Information Security Continuous Monitoring (ISCM), Continuous Diagnostics and Mitigation (CDM) program as defined by NIST 800-137 maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM activities include: Monitoring for control effectiveness, monitoring for changes to systems, monitoring environments of operation.
- **Federal Risk and Authorization Management Program (FedRAMP)** - RPA implementations within FedRAMP cloud authorized systems, or RPA services delivered by a FedRAMP hosting infrastructure, including SaaS, PaaS, or IaaS, may be able to use a FedRAMP authorization. The agency must carefully determine that the 3PAO assessment addresses security and privacy risk posed by the RPA implementation. The client agency's RPA data security, privacy, compliance, liability, and resilience may also become a consideration at the Cloud Service Provider (CSP) and at any third-party providers used by the CSP.
- **Incident Response and Business Continuity**— A repository of all RPA implementations, credentials, and associated applications and environments, and the respective department mappings should updated by the RPA team/custodian for ready reference and distribution to coop planners, business continuity teams and sites, and jump teams in the event of an incident or disaster and subsequent forensics.

CREDENTIALING POLICY

MATURITY MODEL ALIGNMENT

| Start-Up RPA Programs | Emerging RPA Programs | Impactful RPA Programs |
|--|--|--|
| LEVEL 1 <ul style="list-style-type: none">• Human User Credentials• Initial Credentialing Strategy | LEVEL 2 <ul style="list-style-type: none">• Human and Non-Person Entity Credentials | LEVEL 3 <ul style="list-style-type: none">• Non-Person Entity Credentials• Advanced Credentialing Strategy |

Level 1: Credentialing Policy for Start-Up RPA Programs

When beginning an RPA pilot program, many agencies have elected to create automations using the desktop model. In the desktop model, the automation receives systems access through existing human user credentials. Human users receive network access during onboarding through the certificates stored on their PIV or CAC cards. This approach satisfies agency and federal credentialing requirements, and ensure the pilot is implemented with limited cost, delay, and complexity.

Although the requirements of an RPA pilot can be satisfied with human user credentials via the desktop model, it is recommended that RPA programs begin planning for a more robust credentialing strategy shortly after program launch. The Federal CIO Community has not issued authoritative guidance on credentialing for non-person entities (NPEs), leaving individual agencies to create their own policies for RPA.

In terms of applicable federal guidance, OMB Memo M-19-17 states, “agencies shall manage and identify lifecycle of devices, non-person entities (NPEs), and automated technologies such as RPA tools and AI, ensuring the digital identity is distinguishable, auditable, and consistently managed across the agency. This includes establishing mechanisms to bind, update, revoke, and destroy credentials for the device or automated technology.” Existing guidance requires NPE credentials to be clearly distinguishable from human credentials and RPA programs must establish an auditable and well-managed approach to credential management. To date, how best to accomplish this task are left to individual agencies to solve.

It is the recommendation of the RPA CoP that automation credentialing, at the highest level, should be approached and managed the same as credentialing human users. Policies and procedures for granting access to human users have been in place for decades and should be leveraged to credential NPEs. The primary practice for credentialing human users is defined through the Public Key Infrastructure (PKI) Framework in which certificates authenticate users and allow access to websites or systems. The Department of Defense (DOD) uses CAC, while the remainder of the federal governments uses PIV. Access control is achieved via certificates being loaded onto the tokens/cards along with PKI keys according to agency procedures. Prompting mechanisms authenticate access and ensure compliance.

CREDENTIALING POLICY

It is important the security principle of least privilege applies to NPE credentialing, as it would to human users. The RPA program's goal should be to obtain the minimum level of access to applications, systems, processes, and devices required to complete the task automation, and nothing more. In general, RPA automations require two types of access to operate effectively.

- 1) **Service/Network Access** - Access needed to grant an automation an email address and access to network share drives (currently controlled through the PKI Framework - PIV/CAC cards).
- 2) **System/Application** - automations will need access to individual systems with user IDs and passwords.

As an RPA Program looks to set its initial strategy for automation credentialing, it is critical to not only leverage the agency's existing PKI Framework, but also to determine the final RPA technology strategy (e.g., vendor, licensing approach, attended/unattended automations). The RPA program's technology strategy will drive the credentialing requirements:

Credentialing Considerations by Platform Type:

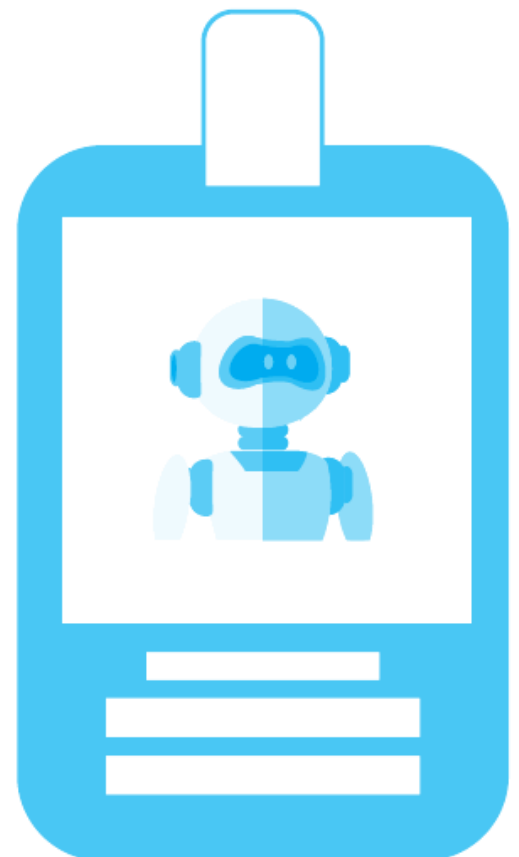
- **Desktop:** The desktop platform requires the use of attended automations. Attended automations leverage human user credentials to access systems.
- **Virtual Desktop (VDI):** The VDI platform can deploy attended and unattended automations. Unattended automations require their own credentials with NPE-specific access certificates.
- **Enterprise Platform:** Allows for an environment using unattended automations requiring credentials with NPE-specific access certificates.

Level 2: Credentialing Policy for Emerging RPA Programs

As discussed in the Technology Infrastructure section of this play-book, an RPA program should use the functionality of a virtual desktop infrastructure (VDI) at Level 2. Automation projects should combine the use of humans credentials with non-person entity credentials. In a virtual desktop, the automation will circumvent single sign on applications by utilizing the users credentials. In this same phase, specific systems should give automations their own credentials (e.g. usernames and passwords).

Public Key Infrastructure (PKI) Framework and Federal Information Processing Standards (FIPS) dictate the requirements governing the credentialing of NPEs. Agency PKI frameworks can be used to issue bot credentials. However, as a best practice, bots should be uniquely identified to easily differentiate between human and NPE users.

Human sponsorship should be required to generate credentials for an automation. Current policies and procedures followed to request and grant usernames and passwords to internal systems for human users should be followed when credentialing an automation with these key differences:



CREDENTIALING POLICY

- **Automation ID:** Naming conventions should be different than human naming conventions to allow for clear differentiation.
- **Social Security Number (SSN):** A SSN is typically required for access to internal systems. A mock SSN range could be reserved for automations or a PKI certification could be assigned as a workaround.
- **Name:** A consistent automation naming convention should apply across the enterprise and should relate to the process being performed by the automation.
- **Supervisor/Manager:** The human sponsor or the automation custodian should be listed as the supervisor for the automation.

When granting NPEs access to systems, the same policies that apply to human users should be applied as it relates to segregation of duties. For example, a human user would not be given access to enter, approve, and pay an invoice. For audit purposes, these same policies should be followed when granting automations access. A Level 2 program, should have documented policies and procedures for automation credentialing, approved and signed by relevant stakeholders, adhering to all audit procedures and segregation of duty requirements.

Level 3: Credentialing Policy for Impactful RPA Programs

As RPA programs evolves from emerging to impactful status, one of the biggest differentiators will be the technology platform used to run automations. As the program grows, it should implement an enterprise framework. In an enterprise environment, attended and unattended automations will likely exist. The unattended automations must become credentialed in order to execute tasks. The same basic framework to getting system access for automation projects from Level 2 should be followed in Level 3.

Significant high-level decisions are needed to drive oversight and provide guidance when implementing RPA. These include:

- Establishing governance will position agencies to monitor compliance with a robust program of security controls as the number of automations deployed increases.
- Larger agencies may need to consider establishing cross-functional governing bodies focused on managing identity. Smaller agencies may only have isolated Program Management Offices (PMOs) focused on limited aspects of identity (e.g., human enrollment or operational PKI services).
- Identity management documentation should be overseen at an enterprise-level and updated to account for new policies and procedures related to automation and NPEs. Specifically, the unique field identifiers and naming conventions used to differentiate NPEs from human users should be in each Agency's policies and procedures.

To ensure program efficiency, the Level 3 RPA program should also monitor the linkage between license management (discussed in Section 3 of this playbook) and credentialing. The program should carefully balance two competing goals - granting each license the least access privileges possible to augment security while also maximizing the ability of the license to run automations 24/7.

MATURITY MODEL ALIGNMENT

Emerging RPA Program

LEVEL 2

- Pilot Privacy Assessment

Impactful RPA Program

LEVEL 3

- Advanced Privacy Assessments
- Documented Policies and Procedures

Level 1: Privacy Policy for Start-Up RPA Programs

Privacy concerns must be considered at the beginning of each automation project. Before a project can be completed, the RPA program will need to adhere to two separate federal mandates: Privacy Act 5 U.S.C. § 552a(e)(10)) and the E-Government Act of 2002, section 208.

Privacy Act 5 U.S.C. § 552a(e)(10)) states that agencies are required to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of PII and to protect against any anticipated threats or hazards to their security or integrity.

The E-Government Act of 2002, section 208 states that agencies must also assess the privacy impact of any information technology that collects, maintains, disseminates, or changes PII.

When beginning an RPA pilot program, it is important to select a use case that, while impactful, limits the complexity associated with IT and privacy approvals. Once the RPA program has selected its pilot use cases for automation and determined how the automation will be run, it may need to engage with its CIO and privacy teams to identify concerns associated with the application of RPA. There are many different tools and methods that privacy offices can use to evaluate the suitability of an automation. The goals of the initial conversation should include the following key discussion points.

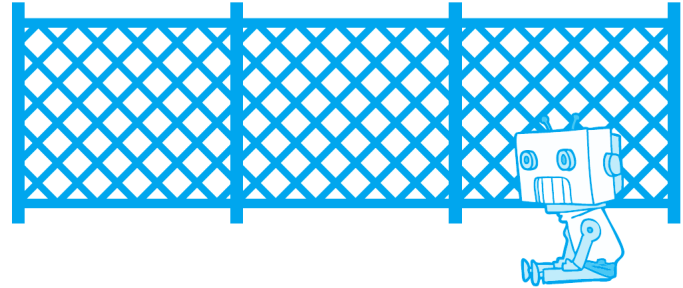
1. An evaluation of the data that the automation will manipulate, share, or access. Is it PII or otherwise sensitive?
2. A determination of the potential privacy risks stemming from the collection, use and disclosure of the information. Does the automation operate across systems or agency boundaries? And, is this an attended or unattended automation?
3. A discussion on how best to mitigate those potential privacy risks using reasonable technical, operational and management controls (e.g. encryption, access controls).
4. Agreement on required documentation to capture actions taken to assess and mitigate risks via the agency's preferred method (e.g., a privacy assessment, POAM, periodic reporting, approvals).

For the pilot program, the use case selected by the RPA program can expedite mitigation of agency privacy concerns, specifically if it avoids PII or otherwise sensitive data. Agency CPOs, SAOPs, CIOs and CISOs all have existing documented procedures for the handling of sensitive data that adhere to applicable federal and agency guidelines. For the purposes of the pilot, the RPA program needs to hammer out an agreement describing how to adopt the existing CIO/CISO approach to the one planned for RPA automation, not for all future automation and data types. Those challenges can be addressed as the program evolves, RPA technology strategy becomes more definite, and the extent of privacy concerns/risks can be more clearly planned and managed.

Level 2: Privacy Policy for Emerging RPA Programs

Once an RPA program successfully deploys a pilot and decides to pursue additional automations, it will need to collaborate with the agency CPO, SAOP, CISO and/or CIO stakeholders to create a formally-approved privacy strategy. The strategy should include of all types of data that an automation might handle, including PII and other sensitive data.

No specific, authoritative federal guidance is currently available on completing privacy assessments for RPA automations. As noted in the previous section, agency CPO, SAOP, CISO and CIO groups should have well documented, existing processes for conducting privacy assessments for other types of automations, system modifications, user access requests, and other change management activities.



The goal for the RPA program is to reach an agreement with the CPO/CISO/CIO as to how best to adapt those existing processes to RPA, such that security and privacy concerns are fully met, while not creating undo burden on the program. The agreed upon processes and procedures should be fully documented, with approval signatures, and available to RPA program staff and stakeholders.

Several agencies have created a formal privacy policy for RPA automations in a two-tier structure. The first tier is a broad review of privacy implications related to the specific systems, applications, and data that the proposed automation will handle, manipulate, store, and send. Some topics included in the initial review are:

- Target system/application descriptions, capabilities, and functionalities.
- Categories of data within the system (by sensitivity level and type).
- Existing system users and proposed additional users.
- Interfaces between target systems and other agency systems/applications.
- Current security and information safeguards monitoring system use and access.

The initial review should be detailed enough to enable CISO/CIO staff to flag all relevant privacy concerns and work with the RPA program to develop mitigation strategies. Once both groups agree to the privacy strategy for the individual automation, signatures and approvals should be collected and documented. It may be advantageous for the CPO/CISO/CIO Office to identify one or two points of contact for reviewing and discussing initial privacy analyses. This will ensure a common approach is followed, and that expertise on issues unique to RPA deployment can be developed within the relevant offices.

The second tier of the privacy review and approval process should entail a more rigorous Privacy Impact Assessment (PIA). The PIA may be required if the automation is handling PII as determined by the PTA. This review builds off initial discussions with the CPO/CISO/CIO and drills into specific data fields, interfaces, and access issues. Each agency should already have a PIA format, but topics specific to RPA deployment could include:

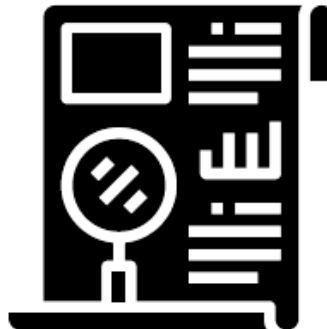
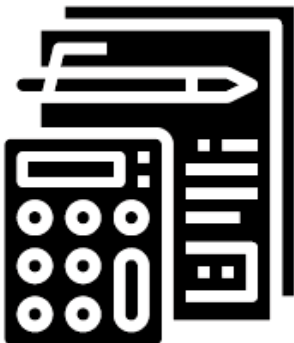
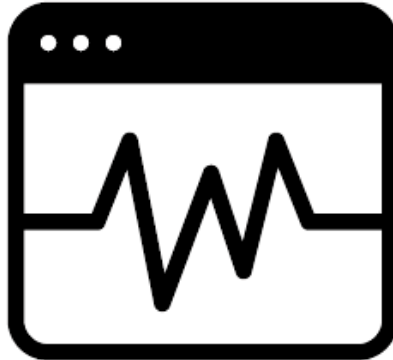
- Established limits on data sharing for relevant fields manipulated/disseminated by the automation.
- Procedures and controls in place to ensure privacy standards are met.
- Monitoring mechanisms and compliance requirements.
- Data quality and potential verification/validation concerns.

SECTION 2

RPA Program Management

MANAGEMENT OVERVIEW

1. Operating Model
2. Program Design
3. Reporting and Business Value
4. Process Selection
5. HR Planning/Impact



RPA MYTHBUSTERS - MANAGEMENT EDITION

Dispelling a few myths and misconceptions about RPA in the federal government ...

1



The best RPA pilot candidates are those with the largest projected ROI.

When introducing a new technology like RPA, ROI can be measured in several different ways including knowledge gained, infrastructure built, and/or capacity created. When planning a pilot, ROI is just one factor to be considered, as agencies should also assess candidate complexity, projected development time, demonstrable impact, and consolidated ownership of process components. A successful small-scale pilot in 90 days can be more valuable than a large-scale pilot in 18 months.

2



Building RPA automations is time-consuming and resource-intensive.

The actual coding of RPA automations should take no more than a week, with a few additional weeks required for testing and vetting. All of the activity around building RPA automations can be time-consuming, including process redesign, security approvals, and technology procurement.

3



RPA is solely intended to cut costs and eliminate workload.

RPA is an effective tool for eliminating manual workloads and associated costs, but it can also be used to improve transaction processing, decrease throughput time, increase accuracy, reduce errors, improve process auditability, and increase productivity levels (number of outputs). Additional benefits of moving employees to high-value work include increased engagement and satisfaction.

4



Building an effective RPA capability depends entirely on contractor expertise.


Contractors can provide significant expertise in starting an RPA program and providing ongoing support. RPA technologies are generally low-complexity, and federal employees can easily be trained to contribute in design, development, and implementation. Tasks like change management, business process expertise, and technology approvals can only be performed by federal employees. Effective RPA programs will likely use both contractors and employees.

5



Employees will fear RPA and not engage with the initiative.

Because RPA automates tasks which often drive dissatisfaction in the workforce (manual, repetitive, low-value), it is often a driver of increased engagement. Federal employees are uniquely mission-driven. With the proper change management and communication strategy, they will see RPA as a means of engaging in more meaningful, mission-aligned work.




AREA 1: Operating Model

Operating Model

The RPA Program's operating model provides the structural framework for **deploying RPA at the agency-level**. Typically designed as a Center of Excellence (COE), the operating model introduces agency-wide standards governing RPA deployment (technology, management, and operations), recommends best practices and decision making frameworks, and ensures adequate controls, risk management, and compliance.

There are various models of RPA COE available for agency implementation. The optimal model will depend on an individual agency's RPA strategy, size and complexity, management culture, organization design scheme, risk tolerance, and many other factors. This section provides common frameworks and mechanisms for implementing an effective operating model for your agency's RPA program, and identifies how those frameworks may change as the program becomes more mature.




AREA 2: RPA Program Design

RPA Program Design

RPA program staff are the critical resources deploying the selected RPA strategy. This section proposes roles and responsibilities for the RPA program as it evolves from a Start-Up organization to a High-Performer. Important roles include the RPA program manager, RPA developers, process support, program support, and performance support.

In addition to providing a proposed staffing strategy, this section also provides internal management approaches to assist RPA programs in maximizing efficiency and effectiveness of operations including key milestones like audit preparedness, controls and standard procedures, and the establishment of formal business services.



AREA 3: Reporting and Value

Management Reporting and Business Value

As detailed in the program design section, a high-performing RPA program can face significant management challenges from the multitude of internal and external stakeholders involved in getting an automation from ideation to deployment. This section provides management and reporting mechanisms that can keep the program moving efficiently and effectively, ensure accountability for performance, and promote operational excellence.

Another important element of managing an RPA program is designing cost and value metrics that enable accurate tracking of program return. This section provides the essentials on business value and cost management, to enable RPA programs to make compelling arguments for ongoing investments.

OPERATING MODEL

MATURITY MODEL ALIGNMENT

| High-Performing RPA Program | Emerging RPA Program | Impactful RPA Program | High-Performing RPA Program |
|--|--|--|---|
| LEVEL 1 | LEVEL 2 | LEVEL 3 | LEVEL 4 |
| <ul style="list-style-type: none"> Pilot Strategy and Goals | <ul style="list-style-type: none"> Strategic Alignment and Leadership Buy-In Capital Planning and Investment Control | <ul style="list-style-type: none"> Oversight and Management Mechanisms COE Design Approaches | <ul style="list-style-type: none"> Fully-Deployed Enterprise COE |

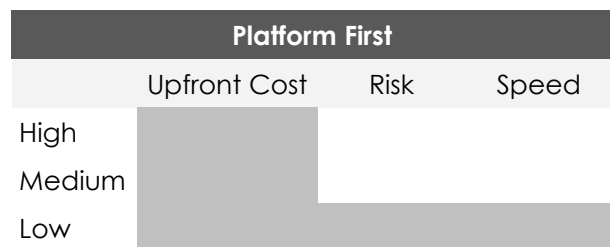
Level 1: Operating Model for Start-Up RPA Program

At the onset, RPA programs should identify the optimal **strategy and goals** for the pilot RPA program. There are currently two prevailing strategies agencies can consider when starting an RPA program. The first pursues the technology platform buildout first, while the second pilots software to gain experience and proof of concept for the technology. The decision on which approach to use determines the level of investment required, the time it will take to deploy the first automation, the required team composition (see program design chapter), and the time required to develop and deploy live automations.

The graphic below provides decision criteria for growing RPA programs to consider in selecting a launch approach. In addition to factors like upfront cost, risk, and speed, the program should consider long-term goals and business priorities. For example, if a program is intended to operate in a centralized COE model that provides agency-wide automation development and deployment, it might be best to use the “platform first” approach to establish a solid basis for a future high-performing factory. Conversely, if the RPA program is the first adopter in its agency, the “experience first” approach might be optimal. This approach allows the entire set of program stakeholders to gain insight into the technology, establish clear guidelines for making it work, and slowly build agency-wide momentum.



Focuses on piloting software and building internal capacity before making a large investment in RPA platform.



Acquires a fully functional RPA platform early in the process minimizing security risk while maximizing software capability.

The RPA CoP recommends all initial RPA programs establish and document aggressive goals, which can take the form of milestones, output measures, and outcomes. These goals serve as useful guidelines for the program to discuss progress with executives, facilitate achieving consensus on program strategy, and encourage ongoing accountability for performance. Example initial program goals are provided in the graphic on page 36.

OPERATING MODEL

Sample RPA Start Up Program Goals



MILESTONE GOALS:

- Our program will implement our first automation within 100 days.
- Our program will acquire and implement an enterprise technology solution within six months.



OUTPUT GOALS:

- Our program will build 10 automations in the first 12 months, and 20 in 18 months.
- The program will support multiple clients across the agency with RPA.



OUTCOME GOALS:

- The program will achieve 100,000 hours of annualized capacity by the end of year one.
- The program will be at Level 4 in the maturity scale within 24 months.

Level 2: Operating Model for Emerging RPA Programs

The RPA Program operating model is the structural framework an agency adopts to drive consistent and effective deployment of RPA. Also referred to as a “Center of Excellence,” the operating model is intended to set agency-wide standards for RPA development and deployment, determine controls and compliance mechanisms, and identify and implement best practices.

A full COE is likely not needed to guide an RPA Program at Level 1 or 2 in the maturity scale, as the program’s automations will likely not have cross-agency impact or involve more than one business unit. If that is not the case, the COE may need to be implemented sooner in the program’s evolution.

Typically, a Level 2 program should focus on setting an effective program strategy, obtaining leadership buy-in, and establishing agreement around program costs. Best practices for achieving these initial governance steps are provided below:

Strategic Alignment and Leadership Buy-In

1. Establish clear, targeted goals for the RPA program in terms of scope and desired outcomes.
2. Ensure alignment between RPA program’s goals, organizational mission, and customer priorities.
3. Develop strategic metrics (tips and methods in the business value section of this playbook) defining success for the RPA program.
4. Create a high-level RACI chart establishing clear roles and responsibilities within the RPA program and other relevant stakeholders within the agency. Achieve approval from all stakeholders.
5. Develop an RPA communication strategy for the appropriate stakeholders (leadership, management, operations, and end users).
6. Roll out the RPA communication strategy and gain leadership buy-in for the program’s vision.
7. Refine the RPA organization and operating structure as needed to align with the stated vision.

Capital Planning and Investment Control

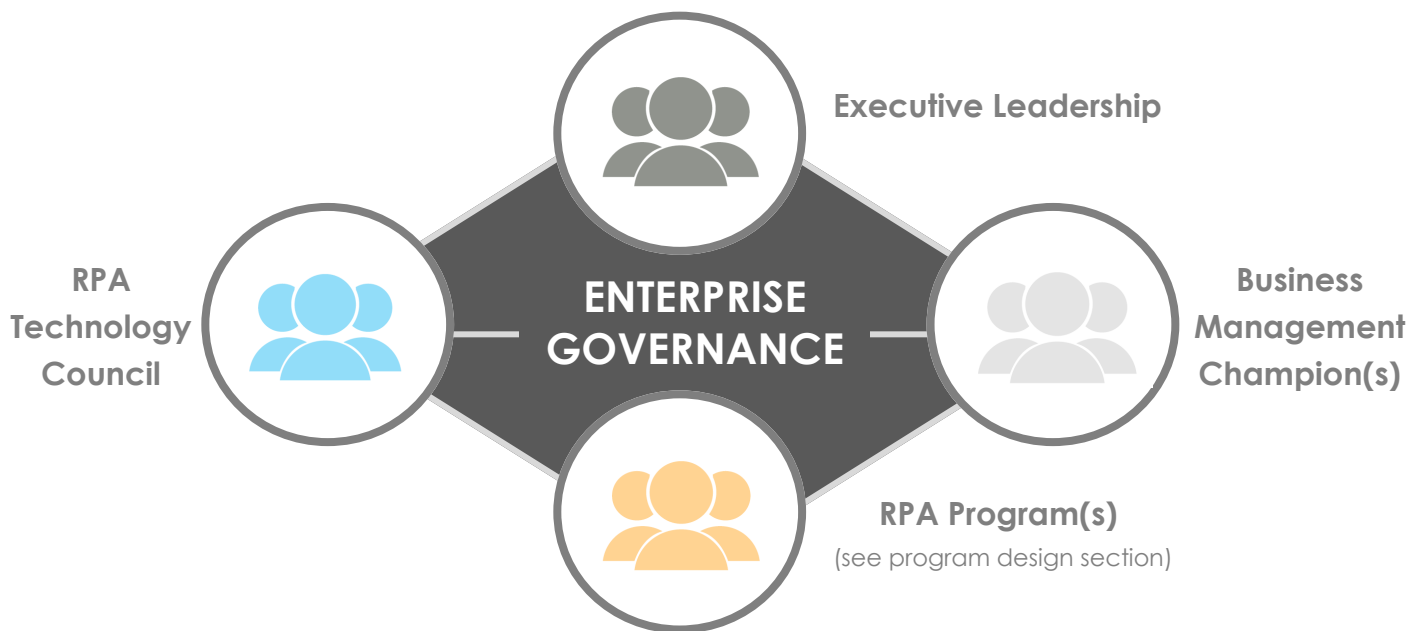
1. Determine the RPA Program’s investment needs in alignment with the executive-approved vision and conduct investment analysis on options (considering enterprise architecture/agency IT policy issues).
2. Ensure the RPA investment strategy aligns with the operating model and will enable the program to meet its intended outcomes (e.g., technology, contracting, resources).
3. Identify potential funding models that align with the Program’s intended outcomes.
4. Achieve buy-in with all relevant agency stakeholders (e.g., OCFO, CIO, Executives, Business Units).
5. Complete budget development based on OMB Circular A-11 Framework.

OPERATING MODEL

Level 3: Operating Model for Impactful RPA Programs

Oversight and Management Mechanisms

Managing an RPA program effectively requires oversight mechanisms that can set a clear strategy, identify ongoing operational risks, establish effective controls, and expedite the deployment of RPA within the agency. The Community of Practice recommends three separate management mechanisms; C-Level executives to drive enterprise RPA strategy; business management champions to prioritize and align RPA efforts; and, RPA technology councils to guide acquisition, deployment, and compliance. The exact contours for how these three management mechanisms should be designed will vary within each agency, and could include creating a formal council or body. The graphic below provides an introduction to each oversight mechanism with initial responsibilities.



| Organization | Membership | Roles |
|---------------------------------|---|--|
| Executive Leadership | Senior representatives from the Executive, CFO, CIO, COO, CISO, privacy officer, and primary business units). | <ul style="list-style-type: none"> Maintain RPA program alignment with agency mission, goals, objectives, and priorities. Facilitate RPA program success including investment funding approaches, project sponsorship, and troubleshooting of executive issues. Promote organizational adoption of RPA. |
| RPA Technology Council | Program management from the CIO, CISO, Privacy Officer, and the RPA Program Manager. | <ul style="list-style-type: none"> Develop consistent agency-wide approaches to technology incorporating federal best practices and compliance. Setting agency-wide technology policies (security, credentialing, and privacy) and agreeing on compliance mechanisms. Designing agency-wide RPA technology infrastructure solutions, vendor/provider options, and procurement vehicles. |
| Business Management Champion(s) | Program management from the primary business units and the RPA program manager. | <ul style="list-style-type: none"> Align business needs and priority initiatives with current and emerging RPA Program capabilities (high-level opportunities). Facilitate the rapid development and deployment of automations, including removing managerial and technical challenges. Promote honest discussions about cost and allocation of resources to fund desired RPA automations. Act as "RPA" ambassadors across the agency. |

OPERATING MODEL

Level 3: Operating Model for Impactful RPA Programs

COE Design Approaches



GOVERNANCE MODEL 1: Centralized

Distinguishing Features:

- The COE is established within one executive office that serves the entire agency.
- The COE manages the entire lifecycle of RPA development from ideation to deployment.
- Customer offices provide process SMEs, testing support and assistance identifying opportunities.

Scenarios for Deployment:

- Agencies with a low-risk tolerance, and a desire for centralized roll out and management of RPA.
- Agencies with only one existing RPA program at a high level of maturity.
- Agencies with centralized IT management and systems.

AGENCY-WIDE DEPICTION

COE - Oversight

Agency-wide standard setting, RPA strategy, investment strategy, performance measurement, technology policy, human capital/workforce planning and reskilling, and compliance.

COE - RPA Program

Automation Development, Testing, and Implementation, License Management, Ongoing Maintenance, Training, and Change Management.

Customer Offices

Process SME, User Acceptance Testing Support, Opportunity Identification



GOVERNANCE MODEL 2: Federated

Distinguishing Features:

- The COE is established within one executive office that provides standard-setting, policy, and overarching management.
- RPA programs work under the COE throughout the agency and can create automations for customer offices if desired.
- Requires close collaboration between the COE and RPA Programs.

Scenarios for Deployment:

- Agencies with strong and well-resourced bureaus/offices.
- Agencies seeking a balance between centralized management and office-specific automation creation/deployment.

AGENCY-WIDE DEPICTION

COE Oversight (COE O)

| | | |
|-------------|-------------|-------------|
| RPA Program | RPA Program | RPA Program |
|-------------|-------------|-------------|

| | | |
|----------------------------|----------------------------|----------------------------|
| Customer Office (Optional) | Customer Office (Optional) | Customer Office (Optional) |
|----------------------------|----------------------------|----------------------------|

| | | |
|----------------------------|----------------------------|----------------------------|
| Customer Office (Optional) | Customer Office (Optional) | Customer Office (Optional) |
|----------------------------|----------------------------|----------------------------|



GOVERNANCE MODEL 3: Decentralized

Distinguishing Features:

- Multiple COEs are established within an agency, with individual RPA program(s) operating under their purview.
- Sub-offices can establish provider/customer relationships as appropriate within the agency.

Scenarios for Deployment:

- Large bureaus or offices exist in the agency with IT systems so unique that standardization and centralized management would be too difficult to achieve.
- Multiple high-performing RPA programs already exist in the agency, with no desire to wind down.

AGENCY-WIDE DEPICTION

COE O COE O COE O

| | | |
|-------------|-------------|-------------|
| RPA Program | RPA Program | RPA Program |
|-------------|-------------|-------------|

| | | |
|------------------------|------------------------|------------------------|
| RPA Program (Optional) | RPA Program (Optional) | RPA Program (Optional) |
|------------------------|------------------------|------------------------|

| | | |
|----------------------------|----------------------------|----------------------------|
| Customer Office (Optional) | Customer Office (Optional) | Customer Office (Optional) |
|----------------------------|----------------------------|----------------------------|

| | | |
|----------------------------|----------------------------|----------------------------|
| Customer Office (Optional) | Customer Office (Optional) | Customer Office (Optional) |
|----------------------------|----------------------------|----------------------------|

Level 3: Operating Model for Impactful RPA Programs

COE Design Approaches (Continued)

As noted on page 38, there are three high-level approaches to establishing an agency COE - centralized, federated, and decentralized. Within these three approaches there are also multiple permutations that can combine management and deployment elements from each model. The exact design and features of the COE will largely depend on an agency's existing structure, RPA program goals, and prioritization of key factors like risk, speed to deployment, controls, and standardization.

The COE should also reflect operational realities, like the degree of standardization and centralized control of IT systems, the resource allocation between bureaus and offices within the agency, and organizational bandwidth to pursue a robust RPA initiative.

Level 4: Operating Model for High-Performing RPA Programs

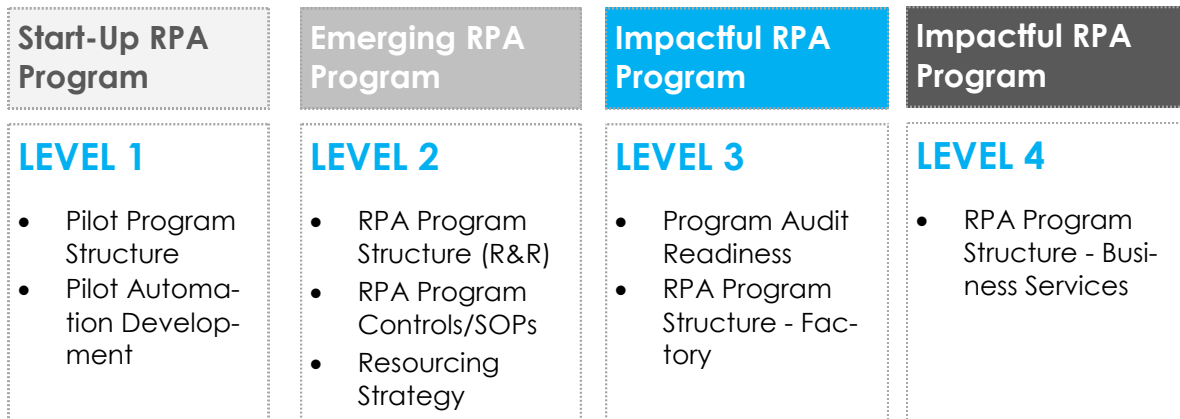
High-Performing RPA programs have enterprise COEs and governance models that are fully-deployed and operate seamlessly. Common techniques to roll out and manage the COE include clearly defined roles and responsibilities, standard operating procedures, change management controls, risk monitoring and mitigation planning, and shared knowledge management and resource libraries. The common hallmarks of a High-Performing RPA program COE are summarized below, with additional information incorporated throughout the remainder of the Management section of this playbook.

Hallmarks of a High-Performing RPA Program COE:

1. **Strategy:** The COE is pursuing an executive-approved RPA strategy governing technology, management, and operations. The strategy is revisited on an annual basis and incorporates business unit priorities, agency management priorities, and federal management priorities.
2. **Performance:** The COE is using a consistent set of strategic and operational metrics (best practices in the business value and management reporting section) to measure the impact and productivity of RPA. Metrics include efficiency indicators, as well as qualitative metrics including throughput, increases in output, quality improvements, error reductions, and new service capabilities.
3. **RPA Investment and Resourcing:** The COE uses a clear, standardized approach to funding RPA initiatives tied to clear performance expectations. Effective resource management is achieved and cost drivers like license management, technology spend, contracting, and employee time allocation are optimized. If the COE adopts a customer service model where RPA programs build automations for other organizations, a transparent cost allocation methodology is in place.
4. **Technology Management:** The COE uses a detailed technology management plan and approach where RPA technologies effectively integrate with the existing IT environment. Common approaches for security, privacy, and credentialing are documented and followed by all RPA programs.
5. **Compliance and Control:** RPA programs follow agreed-upon controls developed at the COE level, automations created follow audit ready business processes, and collaboration with audit groups is planned and carried out effectively.
6. **Operational Excellence:** RPA development and maintenance is efficient and effective, follows best practices, and delivers expected results within ROI bounds set by the COE.

RPA PROGRAM DESIGN

MATURITY MODEL ALIGNMENT



Caveat: The maturity model does not necessitate accomplishing these levels in sequence.

Level 1: Program Design for Start-Up RPA Programs

Pilot Program Structure

Program design during an RPA pilot is often driven by the scope and requirements of the selected opportunity. The proposed roles and responsibilities provided in the figure at right may vary depending on the complexity, duration, and agency-specific technical requirements.

At a high-level, it is important to reflect a few principles in designing the RPA program to support the successful launch of a pilot:

- **Managed Investment** - Requires low levels of initial funding, resources, and the use of staff time. An expensive pilot will likely derail the agency's momentum, and counter the narrative that RPA is a low-cost solution to task automation challenges.
- **Flexible** - Identified resources should be comfortable working across functional responsibilities likely to be divided into separate positions in a larger RPA program (e.g., requirements, technology acquisition, management). The graphic above provides a table of recommended roles and responsibilities for an RPA pilot program, but the exact structure will depend on the complexity, scope, and impact of the RPA opportunity selected.
- **Rapid but Effective** - The longer an RPA pilot takes to be implemented, the less confidence leadership will have in the eventual widespread use of the technology. The pilot program should be resourced to deliver results on a tight timeframe, and to effectively balance two competing interests 1) selecting an impactful use case that provides immediate benefit; and 2) showing the process to achieve that benefit is fast and can be repeated across the organization.

| Pilot Program Roles and Responsibilities | | |
|--|---|------------|
| Role | Responsibility | Allocation |
| Program Manager | The program manager leads the acquisition of pilot technology, collaborates with relevant IT stakeholders to obtain initial approvals, identifies bot requirements, and coordinates development, testing, and deployment (as possible). | Part Time |
| Business SME | The business SME assists the program manager in identifying bot requirements and participates as needed in user acceptance testing. | Part Time |
| Developer | Whether a contractor or Federal resource, the developer leverages the selected technology to program, test, and deploy the bot. | Part Time |

RPA PROGRAM DESIGN

Pilot Automation Development

The RPA program will need to make a decision regarding resourcing development (e.g., coding, testing, deployment) during the pilot phase. The program can either bring in contractor support or train in-house staff to support the process selection and development of initial projects. Contractors will be able to bring expertise and offer lessons learned during the initial pilot phase of a program while in-house staff will need to learn the technology and the selection processes. As a proof of concept, the identified developers, in conjunction with the RPA program and IT leadership, can begin developing a chosen process using the desktop trial version of the agencies preferred RPA software vendor. If the program chooses to train in-house resources, many vendors offer training and continued support during the trial phase.

Level 2: Program Design for Emerging RPA Programs

RPA Program Structure

For agencies looking to evolve their RPA efforts from a pilot to an emerging program capable of producing 5-20 automations, there are three critical elements from a program design standpoint. First, the RPA program needs to add additional capabilities. Second, the RPA program needs to define an initial set of program controls and SOPs. And third, the program must determine its resourcing strategy.

As highlighted in the graphic at right, new capabilities and resources around process assessment and project coordination are required to enable RPA program evolution. The role of process expert is critical in this stage, as the person will lead the assessment of identified opportunities, as well as the design of future state business processes including how the automation fits in the future state process.

Similarly the project coordinator role enables the emerging RPA program to rapidly increase automation throughput. The end-to-end process of identifying an opportunity to deploy an RPA automation includes multiple gates, approvals, and potential challenges. The project coordinator manages that process, including all documentation and milestone tracking, to allow other members of the RPA team to focus on automation creation and program management.

| Emerging Program Roles and Responsibilities | | |
|---|--|------------|
| Role | Responsibility | Allocation |
| Program Manager | The program manager leads the acquisition of technology, the design of privacy, credentialing, and security processes, oversees the development of a robust pipeline, and the management of RPA development and implementation. | Full Time |
| Business SME | The business SME assists the program manager in identifying bot requirements and participates as needed in user acceptance testing. | Part Time |
| Developer | Whether a contractor or federal resource, the developer leverages the selected technology to program, test, and deploy the bot. | Full Time |
| Process Expert | The process expert assesses and validates initial opportunities. The process expert ensures automations are worthwhile and optimally designed. | Part Time |
| Project Coordinator | The path from opportunity identification to RPA deployment can be challenging for an emerging program. The role of the project coordinator is to navigate the process and ensure timely delivery. This enables the developer and PI expert to specialize in their roles. | Part Time |
| RPA Custodian | If the RPA program uses attended automations, the RPA custodian must be trained to launch and manage the automation at the desired frequency. | Part Time |

RPA PROGRAM DESIGN

Level 2: Program Design for Emerging RPA Programs (continued)

RPA Program Controls and Standard Operating Procedures

The second critical element of an emerging program is defining initial controls and standard operating procedures (SOPs). At a minimum, the emerging RPA program should define SOPs for the following areas:




- Privacy Assessments and Compliance
- Security and ATO Completion
- Opportunity Intake and Assessment Criteria
- RPA Development Standards
- Operating and Monitoring Deployed Bots
- Program Roles and Responsibilities
- Program Performance Metrics and Reporting

The other sections of this RPA playbook provide significant detail on topics and issues that should be incorporated in SOP development for the identified areas.

RPA Program Resourcing Strategy

As an RPA program evolves from the pilot phase to an emerging RPA program, a strategic decision will be required on how to resource each function. There are generally three models that an agency can leverage, the contractor, internal FTE, or hybrid approaches. The table below provides a brief description of the pros and cons associated with each of the models.

To date, most agencies have adopted some form of the hybrid model with the balance between contractor and internal FTE tipped by individual program business objectives and staff availability/suitability. The federal RPA COP recommends that agencies consider this balance, and resourcing strategy very carefully. RPA automations represent a new digital workforce and agencies should weigh the long-term impacts of outsourcing all development, management, and control of “digital employees.” Note, too, FTEs reskilled for RPA can come from the business units, and not necessarily IT.

| RPA Program Resourcing Strategy | | |
|---|--|---|
| Models | Pros | Cons |
| Contractor  | <ul style="list-style-type: none"> • Immediate development expertise • Experienced in process selection • Speed to implement • Familiarity with multiple RPA vendor solutions | <ul style="list-style-type: none"> • No institutional knowledge gained • Funds availability • System access, controls, and procurement delays. |
| Internal FTE  | <ul style="list-style-type: none"> • Upskilling of current federal employees to high-value work • Immediate understanding of the internal business processes • Cost-effective approach • Easier systems access | <ul style="list-style-type: none"> • Limited RPA experience • Potential time delay for training • Capacity management (more difficult to adjust for spikes/ebbs in demand) |
| Hybrid  | <ul style="list-style-type: none"> • Immediate business process knowledge and experience using RPA • Can mitigate system access issues • Can balance speed of implementation with lower costs | <ul style="list-style-type: none"> • Contractor utilization - time spent guiding internal staff vs. developing automations • Potential delays due-to additional process handoffs • Requires more agile and dedicated management resources at the program level |

RPA PROGRAM DESIGN

Level 3: Structure for Impactful RPA Programs

An impactful RPA program should be managing a portfolio of 20+ deployed automations with a robust pipeline of future opportunities in development and under evaluation. This increase in demand and the attendant workload will necessitate changes in the RPA program design. Specifically, the program must bolster its intake and assessment processes as well as the automation development and operations functions.

Process Intake and Assessment Capabilities

As detailed in the figure below, the process expert will likely need to become a full-time resource to ensure the program is well-stocked with vetted automation candidates. Although the process expert is not responsible for outreach and marketing (that can likely still be accomplished by the program manager and executives at this phase), there is significant workload in assessing automation candidates, completing process mapping and documentation, designing future state processes, and assisting the program manager in prioritizing projects in the pipeline. Tips and tricks for conducting this work are available in the Process Selection, Assessment, and Improvement section of this Playbook.

The process expert should work seamlessly with the operations team. Approaches for achieving close collaboration vary, and can include work cells of developers, project coordinators, and process experts tackling individual automations as a team - thereby reducing formal handoffs and ultimately automation throughput. Whatever approach the RPA program adopts for internal management, the RPA CoP recommends developer involvement as early as possible with automation projects, avoiding potential delays and rework when the process expert hands off the initial assessment work.

| Impactful RPA Program Roles and Responsibilities | | |
|--|--|------------|
| Role | Responsibility | Allocation |
| Program Manager | The program manager leads the acquisition of technology, monitors compliance with privacy, credentialing, and security processes, leads outreach and marketing, oversees performance reporting and metrics, and monitors RPA development and implementation. | Full Time |
| Business SME | The business SME assists the program manager in identifying bot requirements and participates as needed in user acceptance testing. | Part Time |
| Developer(s) | Whether a contractor or Federal resource, the developer leverages the selected technology to program, test, and deploy the bot. | Full Time |
| Process Expert | The process expert assesses and validates initial opportunities, and ensures automations are beneficial and optimally designed. | Full Time |
| Project Coordinator(s) | The path from opportunity identification to RPA deployment can be challenging for an emerging program. The role of the project coordinator is to navigate the process and ensure timely delivery. | Full Time |
| Program Performance Support | The Impactful RPA program usually manages a robust pipeline of automations in development or under evaluation, as well as 20+ automations in deployment. The Program Performance Support monitors milestone completion across the program and works with the program manager to identify and track targets, metrics, and outcomes. | Part Time |
| RPA Custodian | If the RPA program leverages attended automations, the RPA custodian must be trained to launch and manage the automation at the desired frequency. | Part Time |
| Factory Manager | The factory manager plays a critical role in managing the project coordinators and developers to ensure maximum throughput from the development and operations factory. | Full Time |

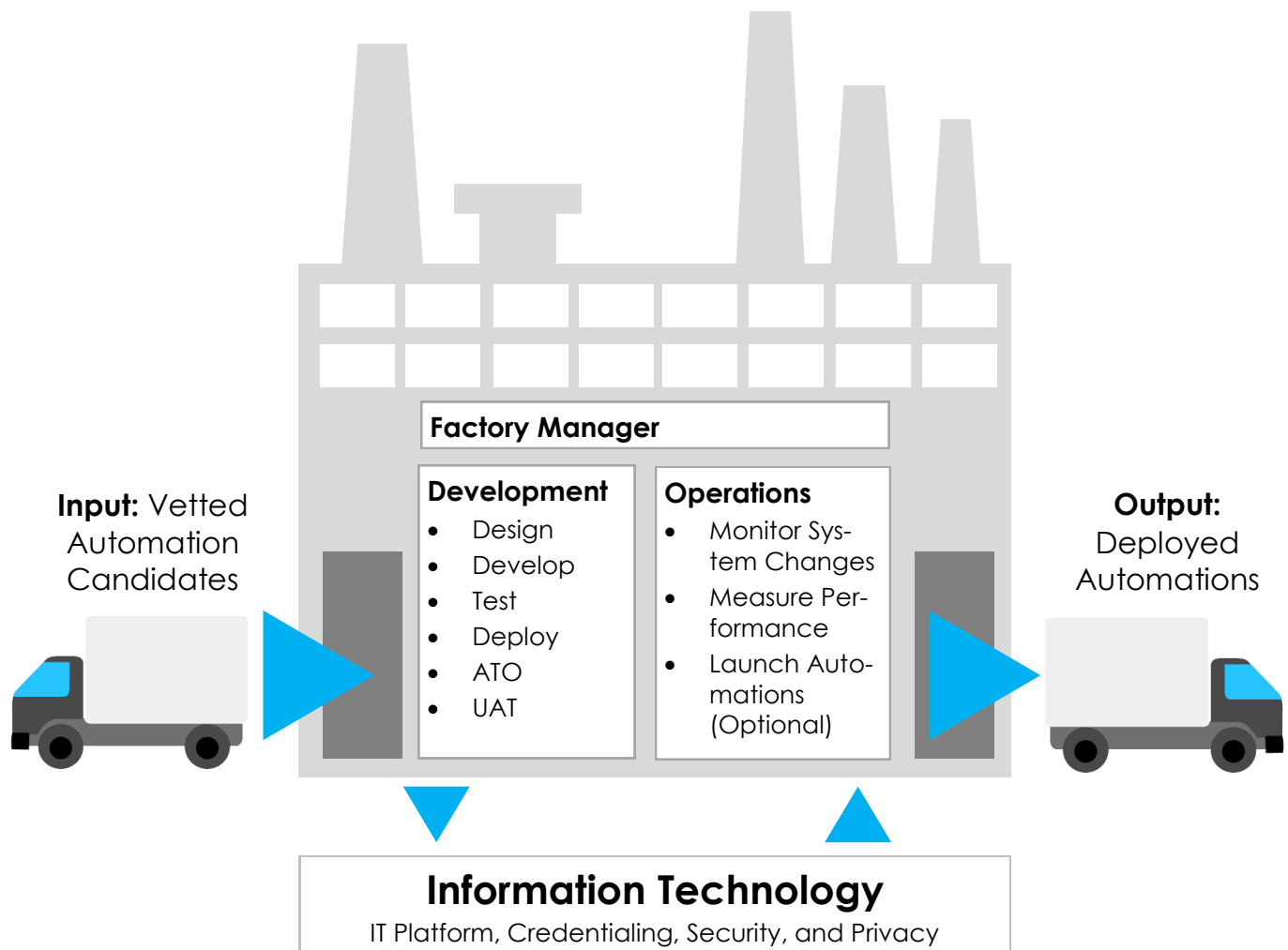
RPA PROGRAM DESIGN

Level 3: Structure for Impactful RPA Programs

Development and Operations Factory

The development and operations workload will surge for an Impactful RPA Program, requiring both new resources and approaches. The role of a “Factory Manager” is critical to overseeing developers and project coordinators in completing the multiple steps, forms, and requirements to get an automation from vetted candidate to fully deployed. The factory manager should monitor the factory’s operational dashboards and/or program metrics, troubleshoot workflow issues, assign projects to developers and coordinators, and monitor program capacity.

The second hallmark of the Development and Operations Factory is the concept of specialization. The workload associated with an Emerging RPA Program will likely allow the same pool of developers to handle both automation development and maintenance (ongoing operations). In the Impactful RPA Program, however, the workload increases to the point that specialization is recommended. Development resources should be focused on designing, developing, and testing automations, while Operations resources should be focused on maintenance - including monitoring system changes, fixing deployed automations, measuring automation performance, conducting quality control and internal controls testing, and launching automations (if an attended scheme is used). The figure below provides a depiction of the Development and Operations Factory.



Level 3: Structure for Impactful RPA Programs

RPA Program Audit Readiness

An “Impactful RPA Program” must perfect its documented controls and SOPs, as it will likely be subject to various internal and external audits and reviews. For example, if the RPA program is responsible for bots that interact with financial systems, the program may be reviewed by A-123 auditors. RPA programs may also be subject to cyclical or ad hoc privacy, security, or other IT audits. These audits or reviews, if they do not provide a formal opinion, are concerned with validating that the RPA program has set sufficient controls and standards, and that the program remains compliant.

Audit readiness concerns the organization’s ability to anticipate, shape, and meet the requirements of auditors or reviewers. As the RPA initiative evolves from a pilot phase to a program phase, it puts in place various controls as program management, project implementation, and bot operations practices are standardized. Audits during a pilot phase are unlikely, as processes, documentation, and roles are still fluid and not easy for auditors/reviewers to test.

A typical RPA audit includes the following steps:

- Identify audit scope - the audit will likely be limited in terms of time period as well as other characteristics of particular bot projects. For example, the review could encompass projects that began development by the first of day of the fiscal year and were deployed by the last day of the fiscal year for bots that interact with financial systems.
- Establish timeline - the audit or review timeline may be influenced by factors outside the control of the RPA program, including the auditor’s contract deliverable commitments and period of performance, as well as other regulations. Auditors usually present a timeline to clarify expectations.
- Establish formal controls - RPA programs may be able to influence the controls that are tested. Auditors will likely want to understand which controls are testable and how they should be tested, as not all auditors possess experience in RPA.
- Sample selection – auditors will select a sample of projects or programmatic procedures to review and request supporting data or access to systems where they may find such information to prove the controls have been met.
- Cure/response period—auditors will provide preliminary findings and generally allow the program to provide additional explanation to justify any deviations from standards.
- Auditor final report – a final report may include findings, recommendations, as well as a formal audit opinion.

Preparing for audits/reviews should begin as soon as the program reaches Maturity Level 3, “Impactful RPA program.” Preparations should include:

- Engage with Auditors - Reach out to the CIO, CISO, and functional C-level executive team (CFO, CHCO, etc) to determine if and what types of audits may include RPA in their scope.
- Prepare resources - Make a roadmap determining when the RPA program may be taxed with additional audit-related duties during the year. Determine how the program will resource the effort.
- Prepare leadership - Make the RPA sponsor aware of upcoming audits and how they may impact the RPA program, and whether there are any known risks or issues that will likely be surfaced.
- Gather and update documentation - As the program evolves, policies and processes can change frequently. Gather existing documentation on RPA program and project management standards. Update the standards to describe current practices. Note the date of the policy or standard change and which projects may have been subject to different or lesser standards.

RPA PROGRAM DESIGN

RPA Program Audit Readiness (continued)

- Educate audit team - take time to step the auditors through your RPA processes, highlighting when certain standards were put in place. Negotiate on a set of agreed-to controls that can be tested, and what documentation will satisfy those controls.
- Internal reviews and testing - conduct internal reviews to determine whether the RPA program should make corrections or adjustments before any audits.

Level 4: Structure for High-Performing RPA Programs

The “Business Services” model provides a structural approach for an RPA program to evolve from impactful to high-performing. In the business services model, the RPA program expands its services and capabilities, allowing the organization to not only be an effective builder and implementer of automations, but also to be a transformative force within its agency.

This model also requires a shift in program orientation and culture. Whereas the factory approach described in Level 3 prioritizes operational excellence, the business services approach also focuses on customer service, relationship management, and agency-wide performance improvement.

| Impactful RPA Program Roles and Responsibilities | | |
|--|--|------------|
| Role | Responsibility | Allocation |
| Program Manager | The program manager leads the acquisition of technology, monitors compliance with privacy, credentialing, and security processes, leads outreach and marketing, oversees performance reporting and metrics, and monitors RPA development and implementation. | Full Time |
| Business SME | The business SME assists the program manager in identifying bot requirements and participates as needed in user acceptance testing. | Part Time |
| Developer(s) | Whether a contractor or federal resource, the developer leverages the selected technology to program, test, and deploy the bot. | Full Time |
| Process Improvement Expert | The process improvement expert in a “business services model” will work with program customers to assess their business challenges, assist in business process improvement and future state design (both related to the automation and more broadly), and support the intake/assessment of bots for the operations factory. | Full Time |
| Project Coordinator(s) | The path from opportunity identification to RPA deployment can be challenging for an emerging program. The role of the project coordinator is to navigate that process and ensure timely delivery. | Full Time |
| Program Performance Support | The impactful RPA program usually manages a robust pipeline of automations in development or under evaluation, as well as 20+ automations in deployment. The Program Performance Support monitors milestone completion across the program and works with the program manager to identify and track targets, metrics, and outcomes. | Part Time |
| Factory Manager | The factory manager plays a critical role in managing the project coordinators and developers to ensure maximum throughput from the development and operations factory. | Full Time |
| Evangelist | The evangelist is a critical part of the “business services model” and is responsible for meeting with program customers to assess their business challenges, identify automation opportunities, and scope opportunities for customers. Essentially, the evangelist is a salesperson closing the deal, and keeping the RPA pipeline full of opportunities. | Part Time |

RPA PROGRAM DESIGN

A critical element of the business services model is the evolution of the program's process experts to process improvement experts. While RPA process experts ensure automations are optimally designed, the process improvement expert ensures the entire process (including the automation) are optimally designed, efficient, and certain to meet customer business outcomes. The process improvement expert is a value-added service for RPA program customers - working in an advisory capacity that transforms an identified thorny business challenge into a set of automation requirements that the RPA Factory can quickly develop and deploy.

The second critical element of the Business Services Model is the addition of sales and marketing capabilities - the Evangelist. This role contains elements of a sales professional, marketer, and customer

relationship manager, but is largely intended to work with RPA program customers to identify opportunities for automation. This would include tailored meetings to discuss a customer's business challenges, assess the viability of RPA as a solution, and develop scope statements. In the same way a sales professional closes a deal, the Evangelist is responsible for generating interest, securing customer buy-in and permission to proceed, and ensuring the RPA program has a deep pipeline of opportunities.

Business Service #1

Sales & Marketing

- Mature Capability to identify opportunities
- Business Challenge Assessment
- Scoping with Customers

Business Service #2

Intake & Assessment

- Assessment
- Documentation
- Process Improvement
- Project Prioritization

Input: Vetted Automation Candidates from a Robust Pipeline



Business Service #3

Development

- Design
- Develop
- Test
- Deploy
- ATO
- UAT

Operations

- Monitor System Changes
- Measure Performance
- Launch Automations (Optional)

Output: Deployed Automations



Information Technology

IT Platform, Credentialing, Security, and Privacy

MANAGEMENT REPORTING AND BUSINESS VALUE

MATURITY MODEL ALIGNMENT

| Emerging RPA Program | Impactful RPA Program | High-Performing RPA Program |
|---|--|---|
| <p>LEVEL 2</p> <p>1. Cost and Value Management 2. Initial RPA Program Metrics and Implementation Dashboard</p> | <p>LEVEL 3</p> <p>1. Advanced RPA Program Metrics 2. RPA Strategic Communications Practices</p> | <p>LEVEL 4</p> <p>1. Robust RPA Program Operations Dashboard</p> |

Level 2: Reporting and Value for Emerging RPA Programs

Cost and Value Management

Agencies should define cost and value management practices to track ongoing investments in the RPA program. Multiple cost categories must be considered, but Level 1 and 2 programs should focus on incremental costs to expedite and simplify tracking. Incremental costs are expenses associated with choices and can be projected forward, as a direct result of the RPA program. To minimize incremental investments, agencies can repurpose existing staff and capacity. For example, technically savvy staff may feel comfortable piloting RPA vendor software and agencies may possess existing virtual or physical servers with spare capacity to run vendor software. RPA vendors can provide support with software installation, testing, and configuration.

The COP also recommends delineating between startup costs (one-time) and operating costs (recurring) which is helpful for resource planning. It should quickly become apparent that RPA is a comparatively low-cost automation tool. Separating one-time startup costs from ongoing operating costs highlights this fact and helps agency leadership see the compelling long-term value proposition of RPA. Therefore, Level 2 RPA programs should plan and track the following:

| COST | | VALUE | |
|---|---|--|--|
| Startup | Operating | Capacity Created | Number of Automations |
| Examples include: Platform configuration, standing up the program management office, contractor support, and pilot costs. | Examples include: Program management, licensing, hosting, bot O&M, and bot development. | For each automation, the number of labor hours (capacity) created by the automation. | A count of the number of automations in each stage |

Level 2: Reporting and Value for Emerging RPA Programs

Initial RPA Program Metrics and Implementation Dashboard

A Level 2, Emerging RPA Program should begin collecting metrics to accurately describe program performance and impact. These indicators should align with strategic goals and outcomes set during the RPA program launch. The CoP recommends the following slate of five metrics as the initial performance indicators because they are relatively easy to collect and report and fully capture the program's impact. It is important for the program to capture the same strategic-level metrics from the point of program launch (post-pilot) to enable long-term tracking of trends and performance improvement.

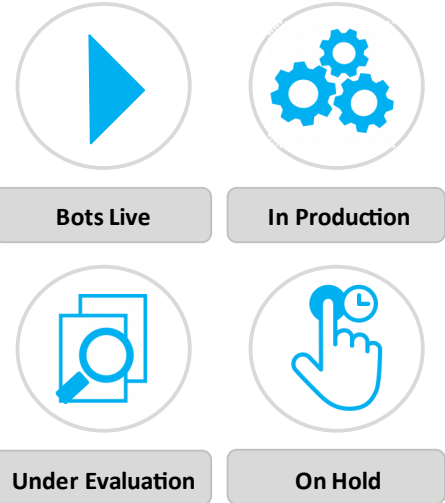
| Metric Name | Type | Description |
|--|----------------------------|--|
| Annualized Capacity Created (in Labor Hours) | Strategic | On a per automation basis, the program should accurately identify the current workload associated with the task (e.g., number of staff performing the task X number of hours per week x 52). This calculation should be performed at the opportunity assessment phase, as it is a critical consideration before a proposed RPA project moves into the development phase. This measure should be captured both as a total for the RPA program, and on a per automation basis, with the goal that both should increase as the program matures. |
| New Capabilities | Strategic (Qualitative) | This measure captures the new capabilities a business unit can deploy because of the successful RPA automation. For example, a business unit could begin auditing new data sets, processing new transactions, or offering new customer data reports. |
| Total Investment Spend to Date | Strategic | The RPA program should keep an ongoing tally of total investment. This metric can be broken down into cost categories (e.g., licensing, technology platform, contracting) that align with agency-specific guidelines or unique information needs. |
| Average Cost Per Automation | Strategic | Similar to the capacity per automation metric, this indicator becomes increasingly important as the RPA program matures. The cost per automation at the pilot phase varies significantly across government with some estimates of \$100 thousand to more than \$1 million depending on the scope, complexity, and technology build out. As the program matures and begins to operate at scale, it should work to decrease this metric and make sure it compares favorably to capacity created per automation. |
| Average Throughput time for an RPA Automation | Strategic | This metric can vary in sophistication, but the RPA program should at least track the project start date (point of opportunity identification) and the project completion date (point the automation "goes live"). As the program matures, an implementation dashboard can be implemented to capture time spent at each phase in the RPA development process (opportunity assessment and vetting, process improvement, documentation, development, testing, deployment) to help the Program make resourcing decisions. This metric should decrease as the program matures. |

Level 2: Reporting and Value for Emerging RPA Programs

Initial RPA Program Metrics and Implementation Dashboard (continued)

With multiple automations in development, production, and under evaluation, the Level 2 RPA program should consider the implementation of a low tech management dashboard. Using a shared technology solution, the RPA program can rapidly create a dashboard that shows where each automation is within the development cycle, identify a single point of accountability, and create basic forecasting tools for project duration and completion.

The implementation dashboard is a particularly useful tool because of the many handoffs in the RPA development and deployment lifecycle. For example, the same staff member will likely not assess the opportunity, complete security approvals, identify technical requirements, conduct process improvement, code the automation, test it, and conduct ongoing maintenance. Without some means of tracking project location and accountable staff, automations can linger at handoff points and the program's ability to rapidly deploy automations will suffer.



Level 3: Reporting and Value for Impactful RPA Programs

Advanced RPA Program Metrics - Strategic

The Level 3, Impactful RPA program should begin to collect and report metrics on the associated benefits of RPA outside capacity created and cost considerations. This will require an expansion of the strategic metrics posited for the Level 2 program above, as well as the introduction of new operational, automation-specific indicators. The CoP has provided recommendations below on specific metrics that Level 3 RPA programs can consider for implementation.

| Metric | Type | Description |
|------------------------------|--------------------------|--|
| Employee Engagement | Strategic or Operational | This measure evaluates the impact of RPA implementation on employee engagement. Captured annually in the Federal Employee Viewpoint survey, this metric can look at high-level engagement and satisfaction scores for the offices in which the RPA program deploys automations, or can drill down into specific questions within the survey. With the addition of more targeted surveying, employee engagement can be measured at the individual automation level for only those staff impacted. |
| Customer Satisfaction | Strategic or Operational | If the RPA program serves clients outside an individual office, it should design customer satisfaction metrics. Either through a passive feedback mechanism or active customer survey, the program should gather data on customer perspectives on speed, quality, and impact of services. Depending on RPA program needs - this can be accomplished at the individual automation level. |

Level 3: Reporting and Value for Impactful RPA Programs

Advanced RPA Program Metrics - Strategic (continued)

| Metric | Type | Description |
|---------------------------------------|-----------|--|
| Average Automation Utilization | Strategic | On average, this metric assesses the percentage of time each automation runs in a 24-hour period. The numerator for the measure is automation run time, and the denominator is total run-time capacity. The program's goal should be to maximize license run time and the number of automations running on a given license. This metric more broadly conveys the cost efficiency of RPA license management and operations. |
| Cost Avoidance | Strategic | In addition to creating workforce capacity, RPA can also help an agency avoid operational costs, a statistic of particular interest to agency executive leadership. This metric captures costs avoided through RPA which can be as diverse as systems retirement, elimination of contractor resources, and consolidation of physical office space. |

Advanced RPA Program Metrics - Operational/Automation-Specific

| Metric | Type | Description |
|-------------------------------|--|--|
| Error Rate (Accuracy) | Operational (Quantitative) | RPA is an effective tool for enhancing compliance and eliminating processing errors. This metric involves a pre and post-intervention assessment of the number of errors in a process sample, and an assessment. An RPA program can quantify this metric both by the number of errors reduced and the cost associated to fix those errors. |
| PII Exposure Reduction | Operational (Quantitative) | RPA technology has the capability to improve an agency's compliance profile. Tasks exposing Personally Identifiable Information (PII) can be automated to limit or eliminate exposure. In addition, automations can continually monitor processing and report suspicious activity. This metric is generally constructed as the reduction in PII incidents. |
| Process Velocity | Operational (Quantitative) | Measures the time that it takes to complete a process. With automations working alongside employees, processes are generally performed much faster. This measure requires a pre- and post-intervention measurement to provide an depiction of time savings. |
| Employee Productivity | Operational (Qualitative/Quantitative) | Assesses employee productivity. While specific to an individual office's operations, this metric can either quantitatively assess pre-and post RPA workload by employee, or can include a qualitative assessment of new products, tasks, and projects employees can complete after an RPA implementation. |
| Strategic Alignment | Operational (Qualitative) | Assesses how an automation is aligned to a larger transformation strategy. In general, this measurement area allows RPA programs to convey how RPA is enabling the agency's broader business goals and strategic priorities. |

Level 3: Reporting and Value for Impactful RPA Programs

RPA Strategic Communications Practices

An Impactful RPA program needs a strong strategic communications capability to support performance reporting, stakeholder management, and program outreach. The CoP recommends agencies plan for communication initiatives in the following areas:

1. **Operations:** The implementation dashboard is an effective tool for managing workflow and communicating automation status/accountability within the RPA program, but it loses some effectiveness when activity is required by external stakeholders. Standardized operations reports should be provided on a frequent basis to external stakeholders that denote actions required and agreed upon timelines.
2. **Knowledge Management and Controls:** As Standard Operating Procedures (SOPs), metrics, program roles and responsibilities, or any other management change takes place, the program will need to create clear and cogent messages for all program staff, and if affected, external stakeholders. It may be useful for large RPA programs to develop knowledge portals or sharing tools to capture all current guidance, SOPs, requirements, and best practices.
3. **Performance:** Process owners, business unit stakeholders, RPA program leaders, and agency executive leadership will want regular performance reporting on the impact and progress achieved through the RPA program. Unfortunately, these stakeholder might also want different types of information. The RPA program will need to effectively determine stakeholder information needs and create tailored reporting solutions using some of the metrics described in the previous section.
4. **Change Management:** A Level 3 RPA program will likely engage in automation efforts having significant impact on stakeholders across their agencies. Change management communications will be needed to inform impacted leadership and staff of the changes associated with automations.
5. **Outreach and Marketing** - As part of the RPA program's efforts to identify automation candidates and potential customer organizations across the agency, it needs to develop visually compelling success cases, impact statements, and automation descriptions.

Level 4: High-Performing RPA Program

In addition to all of the attributes described in levels 1-3 above, the level 4 program should build and incorporate robust and insightful operational dashboard capabilities to manage the development and delivery of automations. Most of the current enterprise RPA platforms possess operational dashboard capabilities built in, with varying features, views, data elements, and metrics. The RPA program should customize these solutions for their information needs, particularly for schedule management, queue management, error logging and mitigation, and capacity management.

The graphic on page 53 provides a high-level sample of some of the metrics and features currently available in RPA enterprise platform dashboards.

Level 2 & 3 RPA Implementation Dashboard



Bots Live



In Production



Under Evaluation



On Hold



Individual Automations

- Automation-Specific Metrics
- Automation Failure Tracking
- Automation Error Coding and Impact Assessment
- Bot Status (Run time, number of outputs)
- Upcoming Scheduling and Activity Monitoring



Audit Management

- Failure Events by Activity Type
- Activity Audit Trail by Host Machine Type
- Activity Audit Trail by User Name

Level 4 RPA Operations Dashboard Functionality



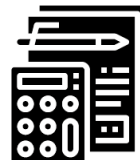
Program Management

- Active User Tracking
- Automation Scheduling and Program-Wide Utilization
- Active Queues and Queue Management
- Bot Velocity and Run Times
- Capacity Utilization (Automation distribution across devices - as applicable).
- License Management
- Program Performance Metrics (automation status, capacity saved, throughput times by development stage).



Device Management

- Device-Specific Metrics
- CPU Utilization
- Memory Utilization
- Hard Disk Drive Utilization
- Forecasted Device Utilization



Workload Management

- Total Capacity Management (time required to complete all automation tasks).
- Queues by Automation Run Time
- Queues by Impact and Average Processing Time
- Queues by Qualitative Factors (e.g., error reduction, improved quality)
- Device Pools by FTE (comparing automation run time against time human operator would take).

AREA 1:

Process Selection, Assessment, and Improvement

Process Selection/Assessment/Improvement

One of the most critical choices an RPA Program must make is which tasks and processes are candidates for applying RPA. This section provides guidance on how to select the best RPA candidates, including pilot opportunity identification, the elements of good RPA candidates, and approaches for conducting suitability, strategic alignment, and impact assessments,

As a program matures, the process assessment and intake capability should evolve from the optimal design of RPA automations, to optimal design of business processes. A robust slate of process improvement capabilities allows

the High-Performing RPA Program to solve agency-wide business challenges and attain broad-scale, transformative impact on operations and performance.

AREA 2:

HR Planning and RPA Impact

HR Planning and RPA Impact

In alignment with PMA CAP Goal 6, RPA automations are intended to support the transition of employee workload from low to high value tasks. Although not the direct responsibility of the RPA program, the program is an important actor in assisting agency leadership in measuring the impact of RPA on the workforce, and planning for future workforce growth and development.

Additionally, the RPA program plays an important role in staff perception of RPA applications within the agency. With a thoughtful and deliberate messaging and educational strategy, staff will see RPA as an enhancement tool, positively impacting their quality of work life balance by removing low value, low satisfaction tasks. In time, RPA can become an important tool in the program manager's arsenal for positively influencing staff engagement and retention strategies.

AREA 3:

Operations Management

Operations Management

At Levels 2 and 3 of RPA program maturity, additional capabilities in operations management need to be deployed, including ongoing testing, maintenance, and optimization of automations. The program needs a robust strategy for ensuring automations stay operational, actively monitoring system changes that can disrupt automation performance, and for managing administrative, technological, security, and credentialing challenges that may cause rework for the RPA program.

The successful operations management program will ensure the program is audit-ready, performs against established operational expectations, improves customer satisfaction with automation performance, and maximizes the program's usage of resources (e.g., license management).

PROCESS SELECTION, ASSESSMENT AND IMPROVEMENT

MATURITY MODEL ALIGNMENT

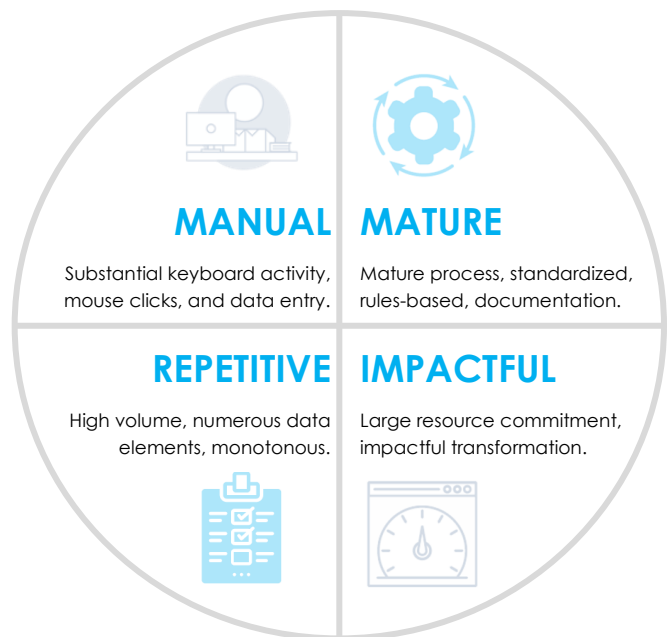
| Start-Up RPA Programs | Emerging RPA Programs | Impactful RPA Programs |
|--|--|--|
| LEVEL 1 <ul style="list-style-type: none"> Pilot Process Selection Pilot Identification Methods | LEVEL 2 <ul style="list-style-type: none"> Initial RPA Candidate Identification Opportunity Evaluation and Prioritization | LEVEL 3 <ul style="list-style-type: none"> Advanced Process Identification Methods Process Improvement Capabilities |

Level 1: Process Selection for Start-Up RPA Programs

Pilot Process Selection

Selecting the correct process is the most critical element of successfully launching an RPA pilot program. In making the best decision, it is important for program leadership to consider the two high-level goals of the pilot program; 1) demonstrating the impact of RPA to transform operations; and 2) demonstrating the speed of RPA implementation as a tool with widespread applicability.

In most cases, pilot processes should be considered “low hanging fruit,” there should be relatively few decision points, intersect with few agency systems, and not handle personally identifiable information (PII). Ideal pilot automation opportunities should come from within the RPA pilot program’s business unit to reduce potential handoffs among stakeholders, and should generally reflect the attributes shown in the figure at right.



Although optimal pilot processes should be low in complexity, they can still provide significant impact. In fact, pilot automation opportunities should solve an important business challenge, including workload elimination, systems integration, improved compliance, or increased throughput. The most important factor in pilot process selection is it must be highly demonstrable. Agency leadership and stakeholders must be able to quickly see the business value provided by the bot, and understand how quickly value can be achieved through the adoption of RPA.

Pilot Identification Methods

Startup RPA programs can begin pilot identification with a high-level scan of their organization's operations, as well as, automations already created within their agency and across the government. The CoP recommends new RPA programs search the following sources for optimal pilot candidates:

PROCESS SELECTION, ASSESSMENT AND IMPROVEMENT

Automations Already Created at Other Federal Agencies - The Federal RPA CoP can be a resource assisting new RPA programs. Many successful pilot projects have already been implemented across the government. The obvious advantage of selecting a proven pilot process, includes lessons learned, clear business value, and the opportunity to receive mentorship from a more advanced RPA program. RPA has been deployed across many functions, including finance, procurement, information technology, mission assurance, and a host of business unit functions.

Common Use Cases of Automations - Examples of common RPA use cases from the private and public sector abound and serve as excellent references for a new RPA program selecting a pilot process. High-level uses case categories include: 1) **Technology Enhancement** (systems integration, enhanced system functionality, and data verification and validation); 2) **Accountability and Audit** (SOP compliance, transaction reviews, automated controls, CAP Management, and risk assessment); 3) **Data Analytics and Reporting** (data reporting, gathering, cleansing, and mining); and 4) **Customer Outreach and Communications**.

Well-Known Existing Business Challenges - Another source of strong RPA pilot opportunities are well-known or persistent business challenges within an organization. These are strong candidates for pilot projects because they likely are already documented to a considerable degree and there is likely a built-in coalition for improvement and transformation. If the entire business challenge cannot be mitigated through RPA, perhaps a piece of the process can be improved through the pilot, assuming the tasks reflect the overarching principles of manual, mature, impactful, and repetitive.

Level 2: Process Selection for Emerging RPA Programs

Initial RPA Candidate Identification

Once the RPA program selects an optimal pilot process for automation, it should be used as an effective tool for proving the RPA concept, and for attracting broader interest in the Emerging RPA Program's services. At its earliest stages, the RPA program should embrace the broad interest it receives and use it to identify a large slate of potential projects. At this stage in the program's evolution it is acceptable to adopt a "what can we automate" mindset to create a large pipeline, demonstrate significant interest in the RPA program, and more broadly to demonstrate interest in transformation through automation. Although this could feel like "drinking from the fire hose," all ideas for opportunities should be captured and documented, as this list will be reduced over time (see evaluation guidance below).

There are various methodologies and approaches a program can implement to build, mature, and maintain an automation pipeline. Organizations should consider using existing leadership boards and end-user groups identifying automation opportunities, as well as establishing additional forums or working groups bringing together potential automation champions. No one technique will be the sole solution to building and sustaining a pipeline of opportunities. It will take a combination of educational outreach, ongoing program success and communication, and active business process evaluation.

The graphic on page 57 provides proposed approaches for Emerging RPA Programs to acquire a strong list of initial RPA candidates, including a brief discussion of pros and cons. These options are not mutually exclusive, as the RPA program could incorporate all approaches simultaneously.

PROCESS SELECTION, ASSESSMENT AND IMPROVEMENT



Questionnaire or Survey

Description: The questionnaire or survey could be sent to all staff (or targeted segments), or could be provided on a website or shared portal as a general intake strategy for the program.

- ^ Great for spreading general awareness of RPA services.
- ^ Will likely produce the greatest initial quantity of candidates.
- ^ Depending on demographics of respondents, could produce candidates with agency-wide impact.
- √ Difficult to provide enough education on RPA to solicit relevant candidates.
- √ Poor candidates require research and follow-up to remove from consideration.



Organizational Consultation

Description: RPA program staff meet with internal or external (customer) organizations to assess business challenges and identify RPA opportunities for the program to help solve.

- ^ Builds close rapport with internal and external stakeholders and provides a great opportunity for knowledge sharing.
- ^ Can result in more targeted RPA opportunities with context needed to expedite development.
- ^ "Bad" ideas can be immediately removed or reshaped into impactful candidates.
- √ Can require significant effort by the RPA program staff and is reliant on an effective facilitator.
- √ Requires collaboration from leadership from internal and external organizations.



Process Consultation

Description: RPA program staff meet with internal or external stakeholders to assess specific business processes, with RPA opportunities generated to improve process outcomes.

- ^ Can result in more targeted RPA opportunities with context needed to expedite development.
- ^ "Bad" ideas can be immediately removed or reshaped into impactful candidates.
- ^ Often a clear business case and willing coalition of stakeholders to expedite deployment.
- √ Can require significant effort by the RPA program staff and is reliant on an effective facilitator.
- √ Requires collaboration from leadership from internal and external organizations.
- √ Opportunities will likely be narrow in scope or within certain offices.

Regardless of the mechanism used to identify RPA candidates - the program must collect and store baseline information on the process to drive prioritization and evaluation. These data fields should be included in a standardized, formal intake form utilized for all opportunities brought to the RPA program. Intake questionnaires can be designed in a variety of applications or using automated tools. Proposed data fields to be included on the intake form are provided below.

1. **General Process Identification:** Including the name and contact information of the individual submitting the idea, the organization and/or office name associated with the process, the business area in which this process is completed, the name of the process, and a high-level process description.
2. **Current Process Metrics:** Including the number of staff/resources used for the process, process volume, frequency, average amount of time currently being spent on the process, current state error rates, and a description of existing challenges.
3. **Systems and Applications:** Including systems involved in the process, system roles necessary to perform process, stability (frequency of changes to the system), instructions for obtaining access, output and input destinations, and data structures and limitations (ex: PII, FOUO).

The RPA team should regularly review and update collection forms/questionnaires and make them available for employees to submit suggestions, through email, on a shared drive, or using other automated tools.

PROCESS SELECTION, ASSESSMENT AND IMPROVEMENT

Opportunity Evaluation and Prioritization

An Emerging RPA Program can find itself with too many automation candidates, where it easily exceeds program capacity and resourcing levels. This is not a cause for alarm, as it generally denotes positive interest in transformation through automation, and suggests significant demand exists for the RPA program's services. However, the program will need to establish a formal set of criteria to ensure the most impactful candidates are green-lighted for development and deployment. In many cases, these decisions will fall under the purview of established governance bodies (e.g., Executive Leadership and Business Management Champions described in the operating model section of this playbook). It is the RPA program's role to provide information and analysis to empower those governance bodies to make informed decisions about RPA candidates.

The Community of Practice recommends three main factors to guide evaluation and prioritization - suitability, strategic alignment, and impact (value). Each factor is detailed below.

| | | |
|--|--|--|
| Suitability Is RPA the right solution to the identified business challenge? | | |
| Areas of Analysis | Attributes - Manual, Repetitive, Stable <ul style="list-style-type: none"> Repetitiveness of Process Frequency Exception Handling Stability of Requirements/Demand Structure and/or Sensitivity of Data Rules-Based Degree of Standardization | Attribute - Complexity <ul style="list-style-type: none"> Number of Locations or Organizations Involved Quality of Process Definition / Documentation Number of Systems and Applications Type of Connectivity Number of Screens and Keystroke Steps Operational Readiness SME Availability |
| Strategic Does the automation candidate align with RPA program and agency strategy? | | |
| Areas of Analysis | Attributes - RPA Program Alignment <ul style="list-style-type: none"> RPA Program Goals and Objectives RPA Program Service Delivery Model and Concept of Operations RPA Program Technology Management and | Attribute - Agency Strategy Alignment <ul style="list-style-type: none"> Agency Mission and Goals Leadership Priorities and Strategies PMA and CAP Goals Broader Agency-Wide Deliverables, Initiatives, |
| Impact How impactful is the automation opportunity to stakeholders and the agency? | | |
| Areas of Analysis | Attributes - Quantitative Value <ul style="list-style-type: none"> Labor Hour Savings Reduction in Cycle Time Increase in Throughput, Process Outputs | Attribute - Qualitative Value <ul style="list-style-type: none"> Increased Compliance/Auditability Enterprise Applicability/Scalability Increased Accuracy |

PROCESS SELECTION, ASSESSMENT AND IMPROVEMENT

Opportunity Evaluation and Prioritization (continued)

To formalize the assessment of the suitability, strategic alignment, and value of RPA automation candidates, the CoP recommends the adoption of a scoring matrix to foster comparative analysis between the opportunities. As denoted in the figure below, a simple weighted prioritization table can achieve this goal. The table assigns weights to the three factors (as determined by the RPA COE), and assigns alignment scores using 1, 3, 7, and 9 for each RPA opportunity. Each COE must determine which elements are included in suitability, strategic alignment, and impact analyses, and if formal thresholds are established for each of the alignment scores.

| RPA Opportunities | Suitability | | Strategic Alignment | | Impact | | Total |
|-------------------|-----------------|-----|---------------------|-----|-----------------|-----|-------|
| | Weight | 2 | Weight | 1 | Weight | 3 | |
| RPA Opportunity 1 | (1/3/7/9 Score) | X*2 | (1/3/7/9 Score) | X*1 | (1/3/7/9 Score) | X*3 | |
| RPA Opportunity 2 | (1/3/7/9 Score) | X*2 | (1/3/7/9 Score) | X*1 | (1/3/7/9 Score) | X*3 | |
| RPA Opportunity 3 | (1/3/7/9 Score) | X*2 | (1/3/7/9 Score) | X*1 | (1/3/7/9 Score) | X*3 | |
| RPA Opportunity 4 | (1/3/7/9 Score) | X*2 | (1/3/7/9 Score) | X*1 | (1/3/7/9 Score) | X*3 | |
| RPA Opportunity 5 | (1/3/7/9 Score) | X*2 | (1/3/7/9 Score) | X*1 | (1/3/7/9 Score) | X*3 | |

Process Documentation

During this phase of the RPA Program, the processes that have been selected for automation should be relatively mature and have well-defined business rules. The goal for designing automations at this maturity level is to optimize the functionality and usability of the automation while aligning it with current state business objectives. Although overarching process improvement or reengineering could eventually become a critical piece of the overall RPA offering, it is not recommended at this phase as it is important to prioritize speed and delivery while the program gains momentum.

To take an approved and prioritized project from the pipeline into development, the RPA factory must begin by translating the business' requirements into an actionable document for the developers to begin the development process. This is typically done in the form of a Process Design Document (PDD). The PDD should be completed before development occurs. It serves as a detailed repository laying out the overall steps and goals of the automation project. It requires a detailed description of the process to be automated while also incorporating a current state and future state process diagram. This document will include keystroke level documentation of the automation project while defining each system that the automation will interface with. This document acts as a formal agreement between the process owner and the RPA program on what will be automated and should be signed off on by all relevant stakeholders. The signed PDD will also be a catalyst for receiving system access approval, as various system owners see the exact steps an automation will take and will be able to assess how the project will impact these systems.

It is recommended as a best practice for the current business owner to perform a recorded walk-through of the process to serve as an ongoing technical reference for the developer. This recording will be instrumental for the developer, as he or she can see all of the systems the automation interfaces with while also detailing the clicks and keystrokes to be incorporated into the automation. Compiling all of these details into an easy-to-understand recording will enable the developer to quickly create the PDD.

Level 3: Process Selection for Impactful RPA Programs

Advanced Process Identification Methods

Alternative Sources of RPA Candidates: Initial consultations with stakeholder groups will likely surface “low hanging fruit” RPA candidates having clear alignment with popular use cases (e.g., data migration, compliance checks). This should be considered a win for a new, Emerging RPA Program as it converts stakeholders into RPA champions and establishes quick program momentum and business value. As the program matures, it should begin adopting a different mindset in creating an opportunity pipeline - from “what can we automate” to “what should we automate.” The problem with low-hanging fruit candidates is that many times those automations do not resolve wider business process challenges.

The Community of Practice recommends the following as sources of data which might unearth more impactful automation candidates: **1) Voice of the Customer Analysis** - asking customers for feedback on their perceptions of business challenges and process impediments. **2) Strategic and Operational Metrics** - analyzing performance data isolating business challenges and root causes. **3) Value Stream Analysis** - mapping current processes and determining workflow issues.

Documented Policies and Procedures: The Impactful RPA program should have a sufficient automation pipeline to necessitate stronger management controls. The program should introduce formal candidate intake and assessment processes, with defined SOPs, resources, and assigned accountability that can be tracked through an implementation dashboard (examples in the Business Value section of the Playbook). These SOPs should include required approval signatures from relevant stakeholder groups and a transparent approach to storing and saving documentation.

Changing the Organizational Culture: As organizations are tasked developing new reporting requirements, implementing new business processes, or adding/modifying compliance procedures, organizations should implement an “automation first” approach. One of the key implementation questions to be answered early is where and how can new processes be designed to take advantage of automation to reduce new workloads, limit manual processes, and ensure additional work is geared toward high-value employee tasks. RPA teams should be a vital part of those discussions, ingraining automation in new business processes and ensuring up front optimal process design.

Level 4: Process Selection for High-Performing RPA Programs

Process Improvement Capabilities

As outlined in the Program Design section, the incorporation of a “business services model” within a High-Performing RPA program demands the development of process improvement capabilities working collaboratively with business unit experts on cross-agency, transformative projects.

The process improvement capability differs from the process evaluation and documentation approach work described in Level 2, because it expands the scope and significance of the tasking. The PDD and documentation efforts seek to optimize automation functionality and translate business requirements to developer requirements, while the RPA process improvement capability seeks to optimize the entire business process for internal or external customer organizations.

PROCESS SELECTION, ASSESSMENT AND IMPROVEMENT

In practice, the process improvement capability would expand the organizational and process consultations described in Level 2 to be more holistic - to address business and challenges in their entirety, not just to determine the applicability of RPA solutions.

RPA programs must make a strategic decision to what extent Continuous Process Improvement capabilities will be integrated, and what CPI methods (Lean, Six Sigma, Re-engineering, Theory of Constraints, etc.) will be used. At a minimum, a handful of basic process improvement techniques can be employed to assess, design, and communicate the steps an RPA automation will follow. In a Level 4 maturity state, CPI capabilities can be integrated throughout the RPA program, from the macro-level process architecture under which all automations reside down to the inner workings of individual RPA projects. Foundational process improvement capabilities include:

- **Facilitation** — capture the various ways in which a task is executed and to facilitate stakeholders to a unified, standard that the automation will follow.
- **Process Mapping** — capture the business processes automations will affect. RPA automates tasks, not processes, so process maps are often not effective at presenting what an automation will accomplish. Rather, process maps capture the business process in which repetitive tasks (automations) reside and captures relationships.
- **Basic Process Analysis** — identify rework loops/defects, excessive cycle times, and wait times in business processes. Once identified, these problems become candidates for automation via RPA.
- **Charter Writing** — facilitate agreement on the automation project and to communicate key aspects of the project (timeline, outcomes, ownership, etc.) to interested parties.
- **Procedure Writing** — document the specific, detailed steps an automation will follow
- **Control Plan or Metrics Plan** — capture the performance metrics the automation is expected to perform. The Control Plan will contain specific corrective actions and accountability for control and improvement.

From these strong foundational process improvement services, an RPA program can augment its skill sets with more advanced techniques. Several key CPI methods should be considered to increase the effectiveness of an RPA program, as follows:

Value Stream Analysis — To capture end-to-end business processes that matter to customers. Value streams represent the core of an organization and how it delivers its value proposition. An effective RPA program will deploy automations in a portfolio model improving business value, not just completes tasks faster. By understanding and measuring value streams, an organization determines if automations are actually increasing throughput, reducing cycle time, and increasing customer satisfaction or if the automations are simply creating backlogs in other parts of the value stream. A mature program will document, catalog, and deploy bots along value streams and will establish performance telemetry based on value streams. RPA programs making the move to Intelligent Automation may also employ Business Process Management tools to connect automations residing within a value stream.

PROCESS SELECTION, ASSESSMENT AND IMPROVEMENT

Theory of Constraints (TOC) - TOC is a method practitioners use to ensure automations are deployed in a balanced portfolio along the value streams mentioned earlier. By using TOC, bots will not create excess capacity and will work together with minimal backlogs.

Lean or Kaizen Events - Lean, Kaizen, or similar Rapid Improvement Events are a highly effective way to expedite the path from problem statement to prototype solution. A skilled CPI expert should be able to facilitate an RPA team with the appropriate stakeholders involved through a series of exercises with the team building the initial version of the automation within three days.

Failure Modes and Effects Analysis (FMEA) - FMEA is highly effective for RPA teams to document the problem points in a process, brainstorm improvements, and score the value of improvements. The FMEA is also a useful method for tracking a portfolio of improvements and leads to easy development of control plans. For risk analysis, the FMEA can also be used as an effective way to assess the potential risks of a future state process relying heavily on an automation or set of automations.

Quantitative Charting and Plotting - The ability to create scatter plots, histograms, and other basic data analyses can be helpful in understanding the impact of defects and delays on repetitive tasks.

Cost of Poor Quality (COPQ) Analysis - COPQ is particularly relevant in the assessment of processes for RPA suitability. COPQ is a method equating issues such as defects, rework, wait times, and slow processing times to a common unit of measure (usually dollars or hours) so the impact of problems can be measured and assessed using a single standard. They can then be assessed against their expected cost of remediation to identify return on investment.

Root Cause Analysis - Root cause analysis is a useful method for identifying the root causes of business problems, ensuring that automations address impactful business challenges. Recommended methods are 5 Whys and Ishikawa.

Quality Function Deployment - To translate problems, ideas, and needs into business requirements and then flow those business requirements to technical and procedure requirements defining the automation or portfolio of automations. QFD is a highly effective matrix-based design technique enabling mature programs to ensure the design of their intelligent automation architecture as well as the functionality of each automation ultimately connect back to business value.

HR PLANNING AND RPA IMPACT

MATURITY MODEL ALIGNMENT

Emerging RPA Program

LEVEL 2

- Employee Engagement and Change Management

Impactful RPA Program

LEVEL 3

- Reskilling or Upskilling Employees Impacted by RPA

Level 2: HR Planning for Emerging RPA Programs

Employee Engagement and Change Management

The term automation can evoke strong reactions from employees, especially the term robotic process automation, as robotics becomes synonymous with job loss and human employee replacement. The truth about RPA, however, it is mostly deployed as task automation, and the software is most often leveraged to “automate tasks not jobs.” The only time RPA could replace an employee is if they only perform one manual, repetitive function, a scenario increasingly unlikely in today's complex federal work environment.

The experienced RPA programs within the federal CoP have found that negative employee impressions of RPA only fester in environments where there is poor messaging and a lack of information about how the software works. With effective communications and change management, RPA programs can dispel employee fears (if any), use RPA as a strong driver of employee engagement, and increase the speed of RPA adoption.

1: Education and Messaging



Element 1: RPA Capabilities - As RPA is a relatively new technology, most employees will likely have no background in its capabilities. RPA program staff can provide a brief primer through existing communication mediums and channels generating enthusiasm around the program and dispel any misinformation about the technology.

Element 2: Benefits of RPA - Federal employees tend to hold strong alignment with their agency's mission, and understand low-value work inhibits their ability to perform tasks aligning with that mission. Viewed in this context, RPA should be a positive driver of engagement because it frees employees from the low-value tasks often fostering dissatisfaction.

2: Staff Inclusion



Element 1: RPA Opportunities - Staff should be included in the RPA opportunities search as SMEs to gain working-level insights into the organization's business challenges. An effective communications campaign should encourage staff participation and acknowledge all contributions. Staff should remain involved in the project throughout to increase feelings of ownership and value.

Element 2: RPA Program Support - Depending on the RPA program's resourcing strategy, staff may or may not play an important role in getting trained as developers, project managers, project coordinators or support staff. For those programs opting out of staff inclusion in program functions, they can still achieve staff participation as organizational champions and experts working with their colleagues to develop RPA opportunities.

Level 3: HR Planning for Impactful RPA Programs

Workforce Planning

An impactful, Level 3 RPA program should consider workforce planning effects from internal and external perspectives.

First, the RPA program must strategically prepare for the future workforce needs of the program itself. The automation workforce includes the roles necessary to run automation programs, including process, operations, technology, and management experts (for more information on exact skill sets refer to the Program Design section of this Playbook). Effective planning should also include an understanding and acquisition strategy for meeting the future needs of the workforce, including the ability to use artificial intelligence tools to complement RPA solutions. The RPA program should take a proactive role in defining its workforce needs and aligning it with agency budgeting and resourcing processes, to ensure the program will have the talent needed to mature the RPA program to meet growth goals.

Second, the RPA program is responsible for collecting and making available data about automations, including those forecasted in the project pipeline, so agency leaders can make plans for workforce impacts and changes. RPA is not a unique phenomenon in the federal government. Over time, many agencies transformed their workforces to retire outdated skill sets (such as, typewriter proficiency). Because RPA occurs at the task level, workforce planning will often resemble an attrition-based strategy, wherein new employees brought into the agency meet new technical requirements, and employees otherwise impacted by automations are assigned higher-value activities.

The CoP recommends working through situations where employees are impacted by RPA with their CHCO or other human resources offices to ensure labor unions are appropriately engaged. Approximately 60 percent of the Executive Branch workforce is covered by bargaining units. As a result, when management decides to reengineer business processes including automation of existing processes, there will most likely be labor relations implications. Agencies hold a right to determine the technology, methods, and means of performing work. However, under 5 USC Chapter 71, agencies have a duty to negotiate proposals regarding the procedures to implement the changes and arrangements to mitigate adverse impact to affected employees.

Reskilling or Upskilling Employees Affected by RPA

As RPA programs mature, they must have mechanisms in place to proactively address the broader effects of RPA on the workforce. While it may not be the responsibility of the RPA program to design reskilling and upskilling strategies, the RPA program is responsible for ensuring the appropriate stakeholders are aware of the potential impacts and take ownership of the topic.

The RPA program should enable appropriate reskilling and upskilling of the workforce by:

- Informing appropriate leadership of data collected during the assessment phase, in order to articulate the potential impacts to workforce for each automation.
- Providing opportunities for interested business users to acquire more technical RPA roles, such as automation custodian, and providing requisite training.
- Following up with organizations with deployed bots to capture metrics and anecdotes showing how human resources have been redeployed to higher value work.

MATURITY MODEL ALIGNMENT

Emerging RPA Program

LEVEL 2

- Operations and Maintenance
- License Management
- Privacy and Security Renewals

Impactful RPA Program

LEVEL 3

- RPA Lifecycle Management
- Code Sharing
- Automation Scheduling

Level 2: Operations Management for Emerging RPA Programs

Operations and Maintenance

During the initial phases of an RPA program, operations and maintenance can be an ad hoc and reactive process. Pilot automations are launched and run until they break. The program staff then works to mitigate issues. The lack of a formal process for supporting on-going testing, maintenance and optimization of automations at this stage is largely due to demand - the number of automations in place does not justify the overhead associated with active monitoring and maintenance. Those resources can be invested elsewhere to gain a better return for the RPA program.

As a program evolves to 10 or more automations, formal monitoring and maintenance mechanisms should be introduced, and strengthened proportionate to increasing program throughput and risk. If the virtual desktop model is followed, an RPA custodian will be needed run deployed automations. The custodian runs automations via the virtual desktop environment and act as the daily user of the automation. These individuals must be trained to launch and manage the automations while determining if the automation is operating in error. There are two prominent reasons why an automation may require additional attention from the business unit or from the developer after is has been put into production:

1. The requirements for a process change; or

2. The automation breaks, typically due to an update to a host application

Requirements Changes: If the requirements to a process change, there should be a formalized process for the business unit to submit a change request for the automation. This process could be in the form of an online submission portal. Once the change request is submitted, it should then be approved by all stakeholders before the change is executed. If a change in the code of the automation is required, there should be a documented amendment to the process design document (PDD) signed by stakeholders reflecting the updates made.

Automation Failures: Automation failures should be a rare occurrence when operating and maintaining an automation catalogue. Automation failures generally result from changes in the production environment including software, system, or front-end updates, or could result from changes in credential requirements.

OPERATIONS MANAGEMENT

To properly plan for changes in the production environment, the RPA COE should document a detailed list of all software, systems, front-ends, and credentials required for the automation to perform its tasks. These details should be tracked at the deployment of each automation and updated as required. To stay ahead of the curve, the RPA PMO should stay in regular contact with the business users to track impending changes. This allows the development team and the business unit to plan appropriately and ensure no loss of automation functionality.

License Management

RPA licensing structures are unique to every RPA software provider. In general, one run-time or robot license will support up to 24 run-time hours per day, seven days per week. For example, if a program has 12 automations in production requiring a total 40-45 hours of run time per day, then the program will need to purchase a minimum of two licenses. There may be different licenses required for attended versus unattended automations, which are all cost factors to be considered before selecting an RPA vendor.

As a best practice, maximize the usage of each license in order to control the overall costs of the RPA program. The length of federal procurement cycles adds increased complexity to managing license utilization, as programs can find themselves with automations ready to go live, and no capacity to deploy. The RPA COE needs to forecast license requirements for up to one year to ensure consistency and seamless delivery when deploying automations. Although it is not recommended to purchase a license until it is ready for use, proper planning is required to closely align bot deployments with license procurement timeframes.

Privacy and Security Renewals

After one year of deploying an automation, the privacy and security office in the agency may require the RPA PMO to recertify the automations. If changes are made to an automation during its one-year authorization cycle, a new privacy threshold assessment (PTA), privacy impact assessment (PIA), or a new authorization to run the automation may be required. If no changes are made to the code during the authorization lifecycle, the existing PTA, PIA, and authorization may only need reverification. These ongoing assessments are critical to mitigating long-term risk.

RPA Development Approach

In designing the development and coding approach for an RPA program, it is important to reference the Software Development Life Cycle (SDLC) as an industry best practice. The SDLC provides a proven methodology for the design, development, and testing of automations with the goal of delivering a targeted solution in an appropriate amount of time.

In the RPA context, the COE will likely determine an agency-wide development approach. The two most common approaches for RPA are structured and agile:



- **Structured:** The structured approach to software development begins with defining the problem, planning the solution, building the solution, checking the solution and then modifying the solution. This linear approach allows for an auditable and repeatable process encompassing the entire lifecycle of a project, but it tends to take longer to build automations and requires more resources than alternatives.
 - **Pro:** Low Risk, Standardization
 - **Con:** Slower, More Expensive
- **Agile:** The agile approach to software development places an emphasis on delivering a solution as quickly as possible. This approach places an emphasis on working in teams and responds well to changing demands for the output. In this approach, the business unit and the development teams need to work closely and effectively bring a project into production.
 - **Pro:** Faster, Less Expensive
 - **Con:** Increased Risk, Lack of Standardization

There are positives and negatives to each approach. If the RPA PMO decides to leverage the use of internal developers, the program must outline its selected approach during training. This sets expectations for the internal resources while also establishing a governance process around the development lifecycle.

Level 3: Operations Management for Impactful RPA Programs

RPA Lifecycle Management

Enterprise RPA platforms must support separate development, testing, acceptance, and production environments for automations - and their dependencies. Bot Lifecycle Management provides a framework for continuous testing and deployment of robots and dependencies in separate software development life cycle environments. This allows automations to seamlessly transition between lifecycle stages defined by the organization, before they are released into production. Implementing role-based access control provides the highest level of security and compliance for automations and is critical as the number and complexity automations increases and the automations address more mission-critical services.

Code Sharing

Because a large enterprise typically uses the same core applications across a number of different business units, mature RPA programs possess the opportunity to scale operations more quickly by creating automations - or pieces of automations - to be reused across the enterprise. For example, your organization's ERP system is likely the target for many automations. Rather than scripting unique login instructions for every automation, a code library of common actions, such as application log-in, can be established to speed development and increase resiliency.

As development begins to scale, and delivery becomes an increasingly important factor, the use of code sharing techniques between developers becomes important to expedite delivery time. Effective code sharing can be achieved through the storage of commonly used snippets of code. Code should be stored in a secured environment accessible to all of the developers. While many of the enterprise platform solutions provide an asset library storing code, the internal developers can also use an internal network drive, if more effective.

Automation Scheduling

To effectively schedule and deploy automations, have a designated individual within the RPA COE work with the business units to decide how new automations will be scheduled on runtime licenses. Unattended automations are scheduled to run at a time of day, specific days and dates, or in response to an external trigger such as an input file landing in a folder. The assigned individual in conjunction with the systems administrator will be tasked with ensuring schedules are being followed and automations are executing as designed. This will also ensure there is no duplication of tasking (automations doing the same thing more than once), which can cause data quality issues. For example, when working with the business unit to create a schedule, it may be decided that a process may need to run at the end of each business day when data is available to be collected. To most effectively use an automation's license, developing a schedule suiting both business unit objectives and the platform constraints is of critical importance.

Operations and Maintenance for Impactful RPA Programs

As an RPA program begins to use the functionality of the enterprise environment, the program may still require an RPA custodian to run a select number of automations that will remain attended. Although some process may remain attended, the RPA PMO should work to migrate as many of the deployed automations to the enterprise platform as possible. The enterprise platform should be managed by a systems administrator to manage and initiate the automations. The systems administrator will also monitor the performance of the automations and will be the first line responder for issue resolution. A formal Operations and Maintenance (O&M) plan should be developed to document the activities required to ensure efficient RPA execution at both the program and automation level.

As an RPA program scales and more automations are deployed into production, the RPA COE should engage with the business units to stay ahead of impending process or systems changes. If there are changes impacting a deployed automation, a formalized and codified change request form should be submitted to the RPA COE. Once the change request is submitted and the proper level of approval is gained, the RPA COE should then assign a developer to assist in making any of the necessary changes.



SECTION 3



APPENDIX

CONTRIBUTORS

Contributing RPA SMEs



JAMES GREGORY

DHS



ANJU ANAND

NSF



FRANK GREENWELL

FRB



VERONICA VILALOBOS

OPM



A'NDREA JONES

HUD



MARIANNE NDEKEY

OPM



MARCELA SOUAYA

GSA

Contributing RPA SMEs



ERICA THOMAS

DOD-OUSD



BO SHEVCHIK

FRB



MARGARET MOON

NSF



KATE MISHRA

HUD



JENNIFER HILL

TREASURY



ELIZABETH MCENTIRE

DOD-OSD



RICHARD SPIEDEL

GSA

Contributing RPA SMEs



SHANG-JEO GAUBLomme

DHS



CHRISTINE GEX

DOD-DASA



TAYLOR ROBERTS

OMB



PAM WOLFE

NASA



David Harris

DOI



Dave Weekley

Treasury

Chair & COP Sponsor

COP Sponsor

Playbook Lead

Lead Author

RPA SME



GERARD BADORREK
Chief Financial Officer
GSA



ANIL CHERIYAN
Director of TTS,
GSA



JIM GEOGHEGAN
CoP Coordinator,
GSA



ANDY STEGMAIER
Vice President,
Management Science
and Innovation (MSI)



NICK SURKAMP
Senior Consultant,
Management Science
and Innovation (MSI)