EXECUTIVE GUIDE

Creating a Robust Controls System for RPA Programs

RPA technologies can achieve transformational outcomes for agencies within aggressive time frames. With such great potential impact, RPA implementations can also create compliance and control risks for agencies. This addendum provides practical insights for federal programs looking to minimize the risks and controls challenges associated with successfully implementing RPA.

Version 1.0 - Published by the Federal RPA Community of Practice

June 25, 2020

LETTER FROM THE CoP CHAIR

Federal Community,

Gerard Badorrek

GSA Chief Financial Officer

Since the launch of the Federal Robotic Process Automation (RPA) Community of Practice (CoP) last year, it has grown from a few dozen RPA enthusiasts to nearly 1,000 members, representing more than 50 federal agencies. The CoP has published an RPA Playbook, held more than 20 knowledge sharing events and webinars, developed a Federal RPA Use Case Inventory, and developed the first automations available for use government wide. Thank you to all the RPA leaders working to make this Community such a success.

During this productive period of growth, our mandate remained the same—to accelerate the adoption of RPA across the federal government. As defined in the CoP's RPA Program Maturity Model, our mission entails developing technology and management capabilities within federal programs to bring RPA production to scale.

While our mission advocates for the rapid adoption of RPA within federal Government, it also calls for smart and effective adoption. We remain clear-eyed about the potential technological, security, and privacy risks that RPA implementations could create. As for many new technologies, existing guidance for RPA is limited. Given the potential for an automation to access personally identifiable information (PII) and the magnitude of transactions an automation can perform, RPA requires strong internal controls.

The CoP can work with agencies to advise on internal control systems that mitigate potential risks. This executive guide, "*Creating a Robust Controls System for RPA Programs",* is a crucial first step. It provides a guide for federal organizations deploying an internal controls regime that monitors RPA program performance, ensures auditability, and reduces IT security and compliance risks. The guide, however, should not be considered prescriptive guidance. Agencies will need to make their own decisions on how to manage RPA within their internal controls framework.

Thank you to our federal RPA Leaders and industry reviewers who contributed to this guide. Your knowledge and dedication are evident, and will help us achieve our mission of rapid, safe, government wide adoption of RPA.

- Gerard

Gerard Badorrek

Federal RPA CoP Chair and Executive Sponsor

TABLE OF CONTENTS

Section	Page
Background and Introduction to RPA	4
RPA Controls System	5
Existing Internal Controls Guidance	5
Unique RPA Risks	6
Key Stakeholder Management	8
Audit Readiness	9
Establishing Robust Controls System	10
Key Control Objectives	10
RPA Maturity Model	11
Level 1 (L1) : Controls for Start-Up Programs	12
Level 2 (L2) : Controls for Emerging Programs	13
Level 3 (L3) : Controls for Impactful Programs	16
Level 4 (L4) : Controls for High-Performing Programs	18
Contributors	19

Introduction to Robotic Process Automation (RPA)

Robotic Process Automation (RPA) is a low- to no-code commercial off the shelf (COTS) technology 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 specific tasks for human users. RPA products vary in their exact capabilities, but all RPA technologies mimic human actions. This technology enables process owners or trained staff to quickly 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.

For government agencies, RPA allows non-IT professionals and process owners to automate a significant share of 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.

RPA Benefits

Agencies can benefit significantly from RPA adoption. First, RPA allows staff to shift from " Low- to High-Value Work" as outlined in the President's Management Agenda (PMA) Cross Agency Priority (CAP) Goal 6. Because RPA automates tasks, not jobs, it creates capacity and reduces staff workload. Employees can then focus on higher value-add work while their "digital assistants" perform standard/repetitive work.

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

Introduction to RPA Controls and Compliance

RPA automations are limited in capability to what they have been programmed to do. From a strict compliance standpoint, they are less risky than human users since they can only do what they are programmed to do. However, RPA automations' access to data, systems, and files, and particularly the magnitude of their throughput can make them a controls challenge for federal programs.

This executive guide reviews the common controls challenges RPA poses and the existing guidance from federal internal controls (IC) canons. With those strong inputs, the Federal RPA Community of Practice (CoP) recommends a strategy for a robust controls environment within government RPA programs. **The Ideas presented in this addendum are not prescriptive or approved guidance. They are recommendations based on current best practices and do not supersede any existing guidance at federal agencies.**

As the topic of internal controls in federal RPA programs is relatively new, the CoP will continue to update this addendum with new lessons learned and best practices. For more information on RPA, please view the RPA Program Playbook, found at www.digital.gov/communities/rpa.

Leveraging Existing Internal Control Guidance for RPA

Most federal organizations adopted an incremental approach to deploying RPA. One drawback of this approach is that RPA program capabilities can eventually outpace control and compliance mechanisms, leaving an agency susceptible to audit, security and compliance, and program risks. As a result, agencies need to ensure that RPA program management and governance standards remain dynamic and change as the organization's RPA capabilities change.

The Government Accountability Office's Standards for Internal Control in the federal government (*The Green Book*) sets standards for an effective internal control system. Most agencies operate mature control environments according to *The Green Book*.

Although RPA poses some unique risks, agencies should draw on existing control frameworks to address RPA implementation risks. As an agency's RPA program capabilities grow, stakeholders from within the agency's RPA, financial management, and IT communities must work together to reduce risks and ensure that controls are documented.

The tenets of *The Green Book* are summarized below:

1

Develop Control System

The foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives.

Actions Required

- Establish program goals - determining what the program wants to occur or not occur.
- Delegate clear authority and responsibility for creating and maintaining controls.
- Develop a documentation strategy.
- Create a program structure that furthers compliance and control roles.

2

Conduct Risk Assessments

Assess the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.

Actions Required

- Develop strategies for risk identification, analysis, and response (accept, avoid, reduce, and share).
- Define objectives in "specific and measurable terms" for operations, reporting, and compliance.
- Identify risk tolerances.

3

Design Control Activities

The actions established through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.

Actions Required

Implement common categories of control:

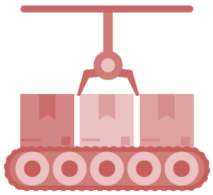
- Management reviews
- Access restrictions
- Recording and documentation standards
- Segregation of duties
- Physical controls
- Measurement reviews and process validation

Unique RPA Risks

Rogue Automation Builders

The simplicity of RPA design, development, and deployment represents a potential risk. Rogue automation builders can operate outside of established norms on software downloaded onto local desktops. Rogue operators pose an especially significant risk in large agencies without an enterprise-level governance structure or a formal approach for obtaining RPA services. Potential groups of independent developers can arise across the agency creating privacy, security, and operational risks for the entire organization. To reduce this risk, agencies can establish a Center of Excellence (COE) to govern access to RPA development and production environments.

Automation Scale



Individual RPA automations can potentially process batches of tens of thousands of transactions. The impact of flawed logic and processing errors will have significant impact. The time and energy required to investigate, evaluate and rework processing errors can create significant workloads for RPA program and business staff. To reduce this risk, take preventative measures. Use a robust monitoring regime with fail-safes coded into the automations, error logs, and standard operating procedures (SOPs) to proactively identify and resolve operational errors.

Error and Exception Management

RPA automations can be programmed to perform transactions or conduct authorizations for millions or even billions of dollars in funds. The RPA Program and internal controls experts must carefully identify risks and acceptable thresholds, also known as "risk appetite". These experts must determine whether the potential liability of an error outweighs the efficiency gain of having the automation process the transaction, authorization, or approval. To reduce this risk, insert human approvals into the RPA workflow at various gates to ensure that an analysts always approves transactions falling into particular categories before moving on to the next major step. While human approvals will decrease process efficiency, they will help avoid significant financial risks or operational failures.

Mismanagement, Waste, and Inefficiency

RPA efforts and programs can be complex to manage, since they require deploying a new technology in a dynamic framework, with only limited emerging governance. The lack of effective controls and standards creates the risk of mismanagement and inefficiency, including inefficient license purchases (types and quantity mismatches), misallocation of RPA Program resources (e.g., developers, business process analysts, program-level management), selection of automation opportunities with limited return on investment (ROI), and inefficient or unnecessary operations and maintenance activities. A formal, documented concept of operations and investment plans ensure that the RPA program optimizes its resources and reduces the risk of waste.

Unique RPA Risks (Continued)

Segregation of Duties

Because RPA is a relatively simple solution and can be rapidly deployed, one individual could fill the role of developer, tester, and operator of the automation, all within a matter of days. However, internal controls best practices require that the development, testing, and operation of automations should be performed by three distinct parties. A certified developer should complete automation development in a controlled development environment. The developer and a tester should complete testing. The process owner (the person who worked the task before automation) should validate the results in a test environment. Once the process owner validates the results and all testing is complete and documented, an RPA systems administrator should move it to a production environment to be run and monitored. The RPA systems administrator should not have access to the development environment where code could be altered or destroyed.

Proactive Automation Maintenance

Since RPA can interface with the front end of any system or application, the RPA program office should engage with IT system owners to learn when changes to systems or applications are scheduled. If required, establish a Memorandum of Understanding (MOU) to ensure all parties involved understand the interactions and relationships. If the RPA program office knows about system updates before release, the automation code can be updated and tested in a test environment. After the process owner validates the updates, the updates can roll into production the same time the system is updated. Routinely check that the deployed automations continue to operate as intended. If the RPA program office doesn't know about changes to a system or application the RPA relies on, the automated processes can break.

Loss of Organizational Knowledge

The longer an RPA automation performs a given task or process, the greater the risk that employees will lose the institutional knowledge associated with completing the now-automated process. This is an exciting problem to have, as it indicates the automation created significant, enduring capacity within the organization. However, if issues arise with the automation, the organization may no longer have a business subject matter expert (SME) who understands the end-to-end business process to correct the issue. Avoid this problem by documenting process knowledge and expertise up front. Capture formal use case documentation and create a common repository for RPA artifacts. Periodically review and update SME roles and responsibilities.

Key Stakeholder Management

For many agencies, RPA fundamentally changes how managers think about workforce strategy, operations, and controls. Take the time to explain to key stakeholders RPA's positive impacts and how a new digital workforce requires updated approaches to internal controls, performance monitoring, and executive oversight. Relevant stakeholder groups vary by agency, but in general, should include the internal audit community, external auditors, executive oversight, and RPA Program-Management.

Each of these stakeholder groups has unique information needs and goals. The RPA Program should use different techniques and approaches for change management activities with each group:

Internal Audit Community - In most federal agencies, there are multiple internal audit groups with varying purviews and investigatory mandates. These groups include the Inspector General, performance management staff, risk management staff, and A-123 staff, among others. Also, federal agencies have many staff members, usually located within business units or administrative groups, responsible for responding to audit requests. Each of these groups will likely be affected by—or interested in—the RPA Program's approach to internal controls and automation monitoring.

Leadership should facilitate knowledge-sharing briefings with the internal audit community members on RPA topics to include (1) introduction to RPA and how the technology works; (2) popular use cases and how they apply to the agency's operations; (3) RPA controls and oversight functionalities, including automation change management; and (4) goals and intended accomplishments.

External Auditors - The RPA Program should limit interaction with the external auditors, responding only to audit requests. This is the case with typical process and technology walkthroughs and observations and provided-by-client (PBC) requests. This addendum provides agencies with proposed control standards to bolster an RPA Program's audit readiness.

Executive Oversight - Key executive leaders such as the Chief Information Officer (CIO), Chief Security Officer (CSO), Chief Privacy Officer (CPO), executive administration, and business unit executives will want to know how RPA is developed, tested, deployed, and monitored within the agency. An RPA program benefits significantly from talking to these key executive leaders early in the program's maturity. Discussions should include plans to develop and standardize related processes and controls. Establishing executive buy-in on a standard set of processes, metrics, controls, and deployment strategy can hasten program development.

Audit Readiness

RPA programs, like other agency operations, are subject to multiple audits and reviews. Develop a strategy with clear goals and objectives to ensure that it is audit-ready.

Audits and reviews include (but are not limited to):

- Office of Inspector General (OIG) financial audits to ensure that automations interacting with financial systems are operating as designed.
- Government Accountability Office (GAO) compliance audits to ensure that the RPA Program complies with established policies and procedures.
- Agency internal control reviews to assess RPA controls' design and operating effectiveness.

Ideally, have complete documentation (digital, paper, or both) for key project decisions. Organize and maintain the documentation to make it readily accessible to auditors. Keep it available for at least one year before archiving.

As the RPA initiative evolves from a pilot to a program phase, establish standard procedures for program management, project implementation and operations. These procedures include documenting key internal controls put in place throughout the RPA life cycle.

Auditors determine the audit scope and timeline. The audit usually includes the following steps:

Key Control Objectives

OBJECTIVE 1:
Auditability

Auditability - RPA programs are subject to audits at the program level and at the individual automation level. Program audits can focus on RPA program goals, objectives, documentation standards and monitoring strategies, internal controls, performance metrics, and results. Individual automation audits can review design plans, systems interactions, data privacy standards, development and coding approaches, and credentialing strategies. A sound internal control program facilitates effective and efficient operations, reliable reporting, and compliance with applicable laws and regulations.

Successful preparation for programmatic audits, financial statement audits, and individual audits require clear and comprehensive documentation and monitoring standards and practices. The program's goal is to ensure auditors can trace data, decisions, and actions for all automations and to establish a definitive strategy with aligned performance indicators.

OBJECTIVE 2:
Security & Compliance

Security & Compliance - Without robust controls in place, RPA implementations can create significant security and compliance risks for IT system owners, IT leaders, RPA Program leader, and partner program leaders. RPA automations are limited to their programmed rules and commands, however, their access to sensitive data, systems, and files requires comprehensive controls and related SOPs in accordance with federal standards, mandates, and controls. Security and compliance controls should ensure data privacy, credentialing, and secure approvals and authorizations. The best security and compliance control program provides RPA leaders, IT leaders, and auditors confidence that the potential risks posed by an RPA implementation are mitigated.

OBJECTIVE 3:
Performance

Performance - A key element of a robust internal controls system is knowing whether the automations are performing as intended and whether the RPA Program is achieving its desired results. Performance-based controls measure aspects of operations management, including uptime and error rates, as well as more traditional indicators like impact validation, cost and ROI, and quality assurance. Proactively monitoring RPA performance effectively and efficiently improves internal control while providing the RPA program with confidence that automations are providing intended value to customers.

Accelerating Government Wide Adoption of RPA

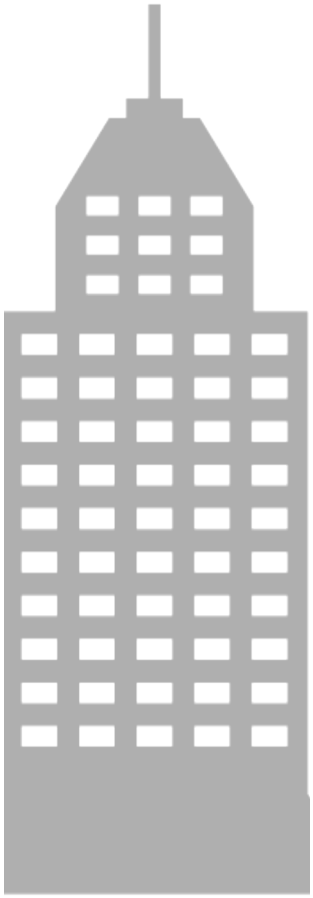
Federal agencies are currently at multiple points in the RPA journey. The Federal RPA Community of Practice (CoP) recently conducted a survey that suggests approximately 25 organizations in the federal government are piloting RPA technology or have a few automations in production. Roughly 10 more programs have five or more automations in production, and five more programs have more than 20 RPA automations already in place.

The maturity model below represents the CoP's vision on how best to measure the evolution of RPA programs. Indicators show agencies' progress, improvements, and how they are scaling their RPA capabilities.

The maturity model is the basis for the program controls and artifacts recommended in this document. The goal is to tailor the robustness of the controls system to the actual risk posed by the operational realities of the RPA Program.

RPA PROGRAM MATURITY MODEL

Start-Up RPA Program	Emerging RPA Program	Impactful RPA Program	High-Performing RPA Program
LEVEL 1	**LEVEL 2**	**LEVEL 3**	**LEVEL 4**
• Pilot bots underway or <5 bots in production. • Fewer than 5k hours of annualized capacity created. • Establishing formal processes related to RPA.	• 5-20 bots in production. • 5k-50k hours of annualized capacity created. • Formally defined initial security, privacy, and ATO policies. • Developing program management, reporting, and process improvement capabilities.	• 20+ bots in production. • 50k-100k hours of annualized capacity created. • Formal ATO, IT security and privacy policies. • Strong program and operations management. • Strong process improvement capabilities. • RPA solutions across multiple functional areas. • Robust pipeline of future opportunities.	• 5-10 bots deployed monthly. • 100k+ hours of annualized capacity created. • COE Model—bots generated from multiple business units. • Intelligent automation capabilities. • Dedicated program management, process reengineering, and development capabilities. • Workforce redeployment, capacity planning, and reskilling required. • Enterprise platform for unattended bots.



Auditability

Element	Description
Controls	1. **Capture Pilot RPA Technology Evaluation Documentation** - Check the requirements of the pilot process opportunity against vendor capabilities, including cost factors, ease of use, technical criteria, and availability of RPA vendor support. This evaluation should also include which vendor solutions may already be on the agency's list of approved technologies. Document this decision and maintain it to support future audits. 2. **Capture Pilot Process Selection Documentation** - Capture where the automation opportunity started and why it was chosen for the pilot. Include how it aligns with the four key elements of a good pilot process: manual, mature, repetitive, and impactful. 3. **Create a Detailed Process Design Document for Pilot Automation** - Complete a Process Design Document (PDD) for the pilot automation. The PDD should document how the automation is constructed; how it is intended to function (i.e., what specific process steps and controls it performs); which systems it impacts; and the strategy for operating and maintaining the automation.
Artifacts	1. Pilot RPA technology evaluation and decision framework. 2. Documentation on pilot process selection. 3. Pilot automation PDD.

Security and Compliance

Element	Description
Controls	1. **Security Approval for Pilot Technology** - Start-up programs will probably not need a broad-scale Authority to Operate (ATO) to begin a pilot. In many cases, initial RPA software approval may be all that is required to begin a pilot program. An authorizing official (AO) can use an authorization decision limited by time and scope as defined in the National Institute on Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2. Options available for RPA pilots could include an authority to proceed, authority to use, interim authority to operate, or interim authority to test. Regardless of the final approval scheme decided with the CIO/CSO, maintain all documentation on the process and decision points. 2. **Approvals for Pilot Automation** - Working with the CIO/CSO, consider establishing a fast-track process for the pilot automation's security, credentialing, and data privacy approvals. Pilot automations are often relatively simple and do not involve sensitive data, this can likely be accomplished through collaboration with relevant stakeholders in the offices of the CSO, CIO, and CPO.
Artifacts	1. CIO/CSO approval to proceed with pilot RPA technology. 2. CIO/CSO waiver to access pilot technology (as applicable). 3. Approval documentation for the pilot automation: credentialing, data privacy, and security, as applicable.

MATURITY LEVEL 1: START-UP PROGRAMS

Performance

Element	Description
Controls	1. **Pilot Strategy and Goals** - Before developing the pilot automation, establish a clear strategy and set of goals and measures to gauge implementation success. These goals can include milestone goals (e.g., the pilot will be live within 100 days), output goals (e.g., the pilot automation will process 10,000 transactions a month), and/or outcome goals (e.g., the pilot automation will create 5,000 hours of workforce capacity). 2. **Pilot Cost and Impact Documentation** - To calculate a reliable return on investment (ROI) for the pilot automation, maintain cost and impact data (i.e., capacity, qualitative benefits, quality improvements).
Artifacts	1. Pilot strategy, goals, and key performance indicators (KPIs). 2. Pilot cost documentation. 3. Pilot impact documentation.

MATURITY LEVEL 2: EMERGING PROGRAMS

Auditability

Element	Description
Controls	1. **Define RPA Program Roles and Responsibilities** - Clearly define roles and responsibilities for all staff and contractors involved in assessment, evaluation, process improvement, development, testing, and maintenance. Identify relevant approvers and oversight groups to ensure that all parties and functions are captured. 2. **Maintain a Consolidated Document Repository** - Collect all documentation and approvals gathered during the RPA lifecycle (assessment to deployment and operations and maintenance) in one consolidated repository, organized according to approved conventions. 3. **Ensure Standard Naming Conventions** - Name all RPA automations with a unique ID, according to a standard naming convention. This unique ID will improve monitoring of activities within systems. 4. **Deploy Standardized Assessment and Development Documentation** - Use standardized assessment and development documentation which can vary based on RPA program customer strategy. Include an opportunity questionnaire or survey, notes from organizational consultations, opportunity evaluation and prioritization matrices, a PDD, and system interaction documentation.
Artifacts	1. Narrated video or detailed SOP of the approved automation in operation. 2. Program wide, standardized PDD. 3. Data privacy approval. 4. Program wide, standardized system owner approval form (if necessary). 5. Formal strategy and naming conventions for automations. 6. Opportunity assessment questionnaire or survey results. 7. Opportunity evaluation and prioritization matrices and analysis.

Security and Compliance

Element	Description
Controls	1. **Retain Technical Requirements and Vendor Selection Documentation** - Document and retain technical requirements and evaluate software for the initial vendor selection process. If required by agency procurement policy, conduct and document a thorough vendor assessment before any procurement is initiated. 2. **Achieve Technology Solution Security Approval** - With CIO, CISO, and CPO approvals, test the selected software. If it receives security approval, place the software on the approved agency software list and keep the approval documentation. 3. **Keep Environments Separate** - As part of the Software Development Life Cycle (SDLC), separate development, testing, and production environments. After concluding development and testing, move the code to a centrally managed production environment. Do not allow ad hoc changes or alterations. 4. **Keep Duties Separate** - Clearly define duties so automation developers are not also responsible for daily operations. Train whoever is running the automation (RPA custodian or systems administrator) before deployment. 5. **Use a Standard Approach to Individual Automation Approvals** - To comply with federal security mandates, agency security teams may require that each automation receives approval before granting permission to be deployed into production. This process can require a number of artifacts to include a PDD and evidence of system owner approval. These documents should be centrally accessible by the RPA PMO.
Artifacts	1. Technology Vendor Assessment (Page 15 of the RPA Program Playbook). 2. RPA Software Approval (LATO, ATO, Approved Software List). 3. CIO and CSO Approved Policies for the RPA Implementation Life Cycle (to include the individual documents required for automation deployment; pages 23-24 of the RPA Program Playbook).

Performance

Element	Description
Controls	1. **Establish an Approved, Clearly Defined RPA Program Strategy** - To gauge whether an RPA Program is performing as intended, strong foundational documents need to convey the following: (A) clear, targeted goals for the RPA program in terms of scope and desired outcomes; (B) alignment between the RPA program's goals and mission and customer priorities; and (C) strategic metrics for the RPA program. Document RPA program benchmarks against other organizations because auditors may ask for this. 2. **Use Standardized Automation Testing Protocols** - RPA testing by internal developers, business users, process owners, and system owners ensures that the RPA program achieves its automation performance goals. While each individual automation may differ in the exact testing protocols used, develop a standard set representing the minimum threshold that each automation must meet before it may be placed into production.

Performance

Element	Description
Controls	3. **Use Standardized Automation Operations Planning Protocols** - Establishing standard operations planning protocols is another critical part of ensuring automation performance. The protocols should list the person responsible for running the automation (RPA system administrator or custodian), how frequently the automation will run, and the expected output or batch size for each iteration. Establish shared and documented performance expectations to improve audit and customer management. 4. **Capture Cost and Value Management Metrics** Capture costs and value management metrics to determine productivity and ROI. Costs can include one-time, start-up costs (i.e., platform configuration, PMO set up, contractor support, pilot costs) and recurring costs (i.e., program management support, licensing, hosting, automation operations and maintenance, and automation development). Basic value management metrics include the capacity created by automating processes and controls and the number of these automations put into production. These data points can establish a compelling narrative for RPA Program successes or identify improvement opportunities. 5. **Report Initial RPA Program Metrics** - Begin collecting metrics on program performance and impact. Align these KPIs with strategic goals and outcomes set during the RPA program launch and can include (A) annualized capacity created in labor hours; (B) new capabilities deployed with workload savings; (C) total investment spend to date; (D) average cost per deployed automation; and (E) average throughput time per automation. 6. **Operations and Maintenance Protocols for Automation Failures** - Emerging RPA programs have 5-10 automations in place. With such limited production, it is often not economical to devote significant resources to operations and maintenance, since RPA automations should, by their nature, seldom break. That said, have documented protocols in place in case an automation fails, including standards for incident investigation, impact assessment, notification and escalation, and developer assignments for remediation.
Artifacts	1. RPA Program strategy, goals, and key performance indicators. 2. RPA Program Capital and Investment Control Plan. 3. Program wide, standardized automation test plan. 4. Program wide, standardized automation operations plan. 5. Cost and value management metrics, documentation, and data sources. 6. Initial RPA Program metrics and data sources. 7. Basic operations and maintenance protocols.

Auditability

Element	Description
Controls	1. **Carefully Manage Developer Access Credentials** - As the RPA program completes more complex automations, individual developers will likely need specialized credentials to access secure systems and manipulate business-sensitive data. Maintain a log of automation access credentials to ensure adequate program capacity for upcoming projects and maintenance of access safeguards. **2. Ensure Chain of Automation Custody Documentation** - By the time a program reaches Level 3 maturity, the program will have more staff involved in assessment, development, testing, and maintenance of automations. To ensure auditability (and performance accountability), track who is working on which segment of each individual automation. Once the automation is deployed, store historical information on contributors and custodians and ensure the program is following all relevant safety, privacy, and credentialing regulations. 3. **Build and Maintain a Comprehensive Controls Document** - Develop and maintain a comprehensive controls document detailing all RPA-related controls applied within the program, the accountable official, and key milestones/metrics associated with each control. This controls document will keep oversight, governance, and audit groups informed of program-level risk mitigation and compliance activities. 4. **Ensure Adequate Audit Logging and Tracking** - The exact audit logging and tracking approach will likely vary within each RPA program depending on the vendor and deployment strategy such as Virtual Desktop Infrastructure (VDI) or enterprise platform. Work to ensure that the audit logging and tracking function provides (A) identification of errors and alterations; (B) documentation and detailed information on automation errors and alterations; and (C) centralized, protected storage to ensure no tampering with audit logs. 5. **Determine Governance Strategy and Operating Model** - As described in the Federal RPA Program Playbook, there are many options for developing a governance strategy and operating model. To establish a robust internal controls system, document governance roles, standard compliance operating procedures, and critical metrics executive leadership and oversight groups have developed.
Artifacts	1. Developer/RPA Program Staff Access Credentials Log. 2. Automation Chain of Custody Information (Historic and Ongoing). 3. RPA Program Comprehensive Controls Document. 4. Audit Logs of Automation Errors and Alterations. 5. RPA Governance Strategy and Operating Model Documentation.

Security and Compliance

Element	Description
Controls	1. **Ensure Centralized Automation Management** - Implementing an enterprise RPA platform allows for centralized storage of code, unattended automations, and provides data analytics for deployed automations. This production environment should be managed by a systems administrator who does not have access to the development environment. 2. **Data Privacy Assessment** - As an RPA program expands, it may be able to automate processes handling Personally Identifiable Information (PII). Have the CPO establish a process to update existing Privacy Impact Assessments (PIAs) for the systems and data with which the RPA software interacts. RPA can handle PII more securely because it limits how many employees require access to sensitive data.

Security and Compliance

Element	Description
Controls	3. **Standardize Account Management/Monitoring of Credentials** - Assign, store, and manage non-person entity (NPE) credentials for all unattended automations. Most RPA software platforms do not comply with federal mandates requiring two-factor authentication for ac-count access. This will require an agency to work with the CIO, CSO, and CPO to integrate third-party software enabling compliant credential management. 4. **Require Data Transmission Agreements** - Before moving data between boundaries, systems, or agencies, the RPA PMO may be required to gain proper authority to transmit the data. When data is transmitted, encrypt it using FIPS140-2/3. 5. **Manage Change** - As processes change or mature, configure a change request process for updating automations to reflect new requirements. A change request should be initiated by the RPA Process Owner for approval by the RPA PMO. Changes in existing automations could include recoding of the automation to meet a new process (reflect updates in the PDD) or migrating from an attended to an unattended automation.
Artifacts	1. Operations plan outlining the schedule for unattended automations. 2. Updates to existing PIAs for high-risk, impacted systems. 3. System Security Plan (SSP). 4. Data Sharing Agreements (DSA), Memorandum of Understanding or Agreement (MOU/ MOA), or Interconnection Security Agreements (ISA) to transmit or access data outside of prescribed boundaries. 5. Standardized RPA Program Change Request Form.

Performance

Element	Description
Controls	1. **Collect and Report on Advanced RPA Program Metrics** - Collect and report metrics on the associated benefits of RPA outside capacity created and cost considerations. This requires expanding the Level 2 strategic metric set, as well as introducing new operational, automa-tion-specific indicators. New indicators can include (A) Employee Engagement (agency-wide and targeted to those affected by automations); (B) Customer Satisfaction; (C) Auto-mation Utilization (program capacity versus actual run times); and (D) Individual Automation Metrics (error rates, reduction in PII exposure, process velocity, and employee productivity). 2. **Ensure Effective Automation Scheduling** - The RPA program should work with business units to determine automation scheduling. Unattended automations are scheduled to run at a spe-cific time or in response to a trigger. Attended automations are run by human operators at an agreed-to frequency. Regardless of which deployment strategy the RPA program lever-ages, it should carefully monitor that automations are on schedule, tasks are not duplicated (data quality issue), and the RPA program is at full capacity (cost-effectiveness). 3. **Establish Proactive Operations and Maintenance Protocols** - Produce a formal operations and maintenance plan that outlines the following: (A) decision criteria for deploying auto-mations (unattended and attended); (B) the systems administrator and staff responsible for monitoring performance; (C) responsibilities for issue resolution and; (D) protocols for proac-tive identification (e.g., systems, processes, and requirements changes).
Artifacts	1. Advanced RPA Program metrics, documentation, and data sources. 2. Automation scheduling strategy and accountability documentation. 3. RPA Program formal Operations and Maintenance Plan.

MATURITY LEVEL 4: HIGH-PERFORMING PROGRAMS

Auditability

Element	Description
Controls	1. **Develop Detailed Documentation During Process Improvement Interventions** - A high-performing, Level 4 RPA program should have effective process-improvement capabilities in place to support clients in broad business transformation. As part of the process improvement intervention, the RPA program should capture the current state process map, process analysis on defects and constraints, procedures and policies, the current process controls, and metrics on the current process. These documents and data serve as important historical artifacts to assess pre- and post-automation performance. 2. **Deploy Robust Plan for Proactive Automation Testing** - Building off of the proactive operations and maintenance protocols and Comprehensive Controls Document described in Maturity Level 3, the High-Performing RPA Program should create a more robust testing and audit plan for its automations. This plan should establish a proactive analysis strategy to ensure ongoing review of automation metrics, performance against established thresholds, errors, and exceptions. Enterprise platform solutions can assist the RPA Program with identification of desired data strata and provide ongoing reporting to relevant stakeholders.
Artifacts	1. Process improvement documentation (e.g., process maps, defect analysis, procedures). 2. Proactive Automation Testing Plan (or monitoring plan). 3. Incident response and business continuity plan.

Performance

Element	Description
Controls	**Robust Operations Metrics Capability** - Most current enterprise RPA platforms have operational dashboard capabilities to manage automation development and delivery. Document data needs and incorporate the areas below into the enterprise dashboard. Together, these capabilities demonstrate a robust operations metrics capability. A) **Program Management** - *How well is the program operating?* KPIs include user tracking, program wide automation utilization, activity queue and queue management, bot velocity and run times, failure events by activity type, audit trails by username and host machine, and license management. B) **Technology Management** - *Is the RPA technology working optimally?* KPIs include device-specific metrics, CPU and memory utilization, total platform capacity management, and device pools by FTE (comparing automation time against human operator run time). C) **Individual Automation Management** - *Are individual RPA automations working optimally?* KPIs include automation-specific performance metrics (detailed in Levels 2 and 3), failure tracking, error coding and impact assessments, bot status (run time, number of outputs), and upcoming scheduling.
Artifacts	1. Operational dashboard requirements, design plan, and capabilities. 2. Operational metrics reporting and analysis (point in time, trending, future forecast).

CONTRIBUTORS

Contributing Federal SMEs

JAMES GREGORY
GSA

KATHY HAMMER
GSA

BERNICE HARVEY
PBGC

ERICA THOMAS
DOD-OUSD

JENNIFER HILL
TREASURY

TAMMIE JOHNSON
TREASURY

Contributing Industry SMEs

SHANE SOWARDS
Senior Manager,
Ernst & Young LLP

AMBER GARIB
Senior Manager,
Ernst & Young LLP

DUC DUONG
Managing Director,
Grant Thornton

JENNIE MELCHIOR
Director,
Guidehouse

SHELLY TURNER
Director,
Guidehouse

Chair & CoP Sponsor	Playbook Lead	Lead Author	RPA SME

GERARD BADORREK
Chief Financial Officer
GSA

JIM GEOGHEGAN
CoP Coordinator,
GSA

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

NICK SURKAMP
Director,
Management Science
and Innovation (MSI)