Intelligent Automation Community

The State of California Intelligent Automation Community provides a collaborative hub for state agencies and departments to automate business processes that involve data intake, data processing and workload management. This community focuses on integrating diverse technologies—including webforms, bulk data files, Robotic Process Automation (RPA), and document extraction (OCR)—to streamline public services.

*The **Intelligent Automation Playbook** serves as a strategic guide, offering best practices and proven strategies to accelerate program maturity. It incorporates lessons learned across the state to help agencies and departments responsibly adopt and scale automation technologies.*

The Intelligent Automation Community's key strategic objectives are to:

- ***Foster Collaboration:** Encourages cross-departmental knowledge sharing to standardize automation efforts.*
- ***Operational Excellence:** Provides frameworks for improving data accuracy and processing speed through automation.*
- ***Responsible Adoption:** Aligns with California's technology adoption goals to ensure safe and secure digital transformation.*

Intelligent Automation Playbook

Intelligent Automation Fundamentals

Intelligent automation utilizes low-code or no-code Commercial Off-the-Shelf (COTS) technology to streamline repetitive, rule-based tasks. By combining various tools and processes, Intelligent Automation optimizes workflows and ensures data remains synchronized across legacy and modern systems.

Key technology solutions within this framework include:

- ***Data Intake:** Web forms for individual transactions and Secure File Transfer for bulk uploads from business partners.*

- ***Digital Transformation:*** *Intelligent Optical Character Recognition (OCR) to digitize paper-based data.*
- ***Operations Management:*** *Robotic Process Automation (RPA) for repetitive tasks and workload management for automated internal assignments.*
- ***Performance Monitoring:*** *Simplified data dashboards to track the status and health of each solution.*

Rather than serving as a workforce reduction tool, Intelligent Automation is designed to empower employees. The California DMV has prioritized these technologies to help staff work faster, meet Service Level Agreements (SLAs), improve customer service, and enhance overall data quality.

Implementing these solutions leads to significant organizational benefits, including reduced human error, data consistency, improved customer service and increased compliance.

Intelligent Automation Capability Areas

Program Technology

Technology Infrastructure - Transitioning to an enterprise grade automation platform is a complex, strategic investment requiring a robust architecture plan to deliver a scalable, enterprise-grade service. While the core automation software itself may remain consistent, the implementation involves moving from single-instance applications to distributed services. The architecture must separate key functions into specialized infrastructure layers, including data storage, messaging queues, compute power, and security services. This ensures enhanced security, easier maintenance, and optimized performance. The enterprise level automation program must incorporate infrastructure replication strategies to achieve high availability, disaster recovery, and load balancing. Additionally, the enterprise grade automation infrastructure is the definitive standard for scaling unattended, attended, and hybrid automation. It enables centralized monitoring and management by integrating seamlessly with existing enterprise IT infrastructure, such as identity management and email services. To ensure long-term success at this scale, the platform mandates rigorous, enterprise-wide standards for security, workflow orchestration, and governance. It also provides robust analytical suites that measure automation performance at every level. Operational dashboards track technical metrics like utilization and error rates, while strategic dashboards provide

leadership with high-level insights into Return on Investment (ROI) and overall program impact. This dual-layered visibility allows organizations to optimize automation health while proving the long-term value of their digital transformation.

Security considerations – Intelligent Automation program must secure a formal approval from the department CIO and/or ISO to utilize enterprise platforms. This process involves a rigorous review of the IT solution, its deployment model, and its alignment with security policies. Some steps include securing the baseline software clearance for the automation platform, future automations often require additional impact assessments, security questionnaires, and technical documentation, and maintaining a close partnership with security branch is essential to prevent approval delays from stalling program growth. Failure to proactively manage these requirements can create significant hurdles for scaling automation initiatives.

Credentials and access management - Intelligent Automation program must collaborate with the department CIO on how the agency will recognize and authentic digital workers with non-person entity credentials. These policies establish a formal process for authenticating users, monitoring access rights and ensuring relevant security policies are upheld. In some cases, agencies have allowed attended automations to inherit the credentials of their human operations. IA programs must monitor access rights and credentials to ensure continued compliance. Each automation must assess credentialing and privacy issues to make sure the automation has the permission levels required to interact with all necessary systems.

Privacy considerations – [To be complete]

Program Management

Team Structure

A high-performing Intelligent Automation team is organized into a **Center of Excellence (CoE)**. This structure centralizes governance, best practices, and technical expertise to ensure automations are scalable, secure, and aligned with organizational goals.

- **Automation Manager / Product Owner** - Provides resources, approvals, and validates process efficiency and other business benefits. Defines the "New World" for their staff. Owns day-to-day operations and business decisions, plans and manages workload distribution. Also manages post implementation automation (fixes / enhancements) pipeline.
- **Process & Implementation Manager** – Acts as the implementation manager, process champion, cutover planner. Defines, manages, and documents process changes. Validates process changes and assists Automation Manager defining the "New World".
- **Product Tester** – Includes business staff that possesses in-depth knowledge about the process. Participates in process and system integration validations. Identifies and logs system errors/bugs during testing validation.
- **Technology Integration Manager** – Facilitates integration process, provides infrastructure for testing, staging and production environments. Coordinates efforts to ensure system compliance on data security policies and standards.
- **Compliance Manager** – Responsible for validating the process automation implementation for compliance to CoE established standards and department security policies. Coordinates with Portfolio Manager to audit and address potential risks and concerns.
- **CoE / Technology Manager** – Initial setup and ongoing operation of the Intelligent Automation CoE. Assists and supports the Compliance Manager in aspects of system and data security measures and controls.
- **Portfolio Manager** – Responsible for end-to-end execution of all Intelligent Automation projects. Participates in project selection, team setup, and project planning and scheduling.

Operating Model

A comprehensive Intelligent Automation operating model is structured across several strategic and technical layers to ensure scalability, and security.

- **Strategic & Organization Layer** – Identify use cases, agree on prioritization, roadmap for future, report out to leadership and executive teams.
- **Tactical Layer** – Automation outcome, benefit tracking and day-to-day management of solutions, change management, identifying automation processes, reviewing for compliance, optimizing and prioritizing use cases.

- **Operational Layer** – Development, maintenance and operations including build and run teams, and infrastructure support. Continuous monitoring of automation components, triaging runtime issues and fixing, fine-tuning, and optimizing. Process compliance, managing security concerns.
- **Access Layer** – Provisioning and deprovisioning rules, setup Role Based Access Controls (RBAC).
- **Segregation of Duties** – Human-in-the-loop vs. automation builder, automation manager vs. automation auditor, automation finalizing multiple tasks previously completed by different profiles.
- **Password Management Layer** – Leverage an application-to-application password management tool (Example: Beyond Trust) to maintain ID and password expiry rules and provisioning.
- **Optimization Layer** – Real-time dashboards for tracking processing volumes, error rates, and actual ROI against projections. Categorize and map automation failures, creating a continuous improvement for exceptions into actionable business insights.

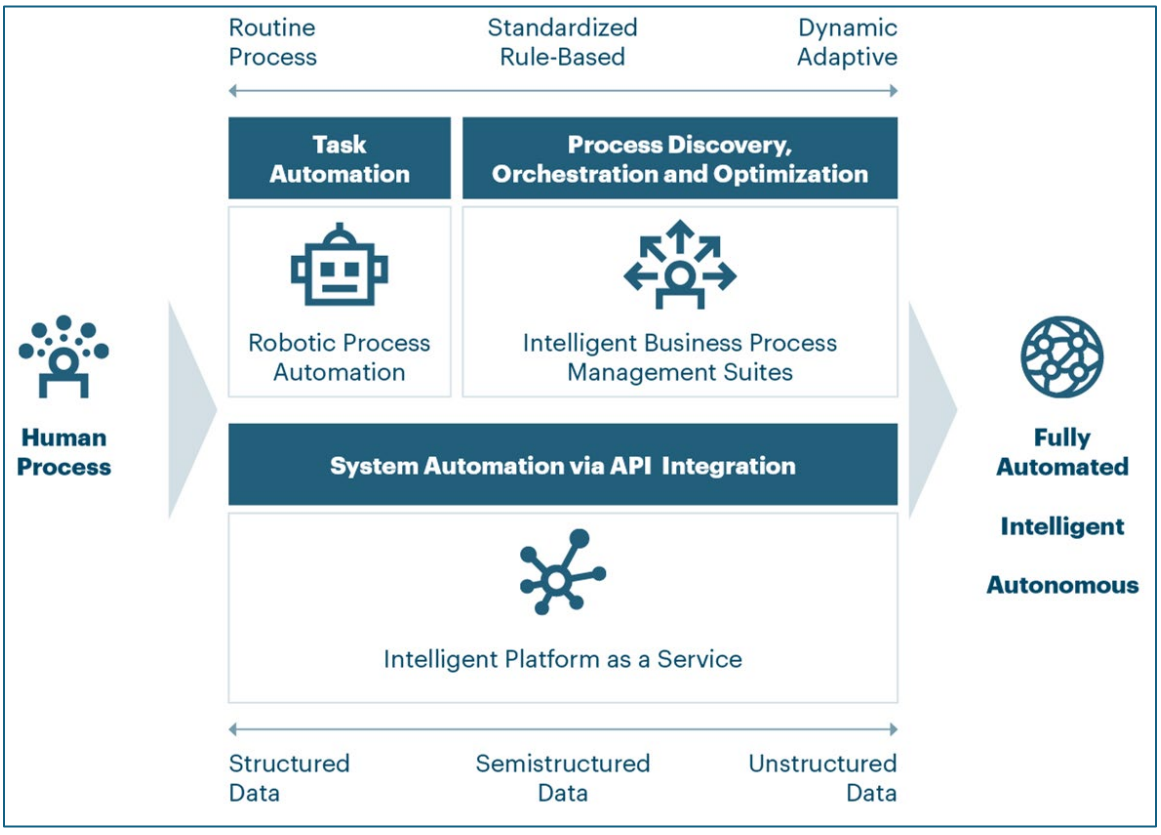
Program Design

Designing a successful Intelligent Automation program requires balancing technical feasibility with long-term business value. Key to success is to focus on strategic alignment, modularity, and governance to ensure automations remain resilient and scalable.

Responsibility Matrix for Intelligent Automation

Activity	CoE	ISD	Business Owner	Process Owner	Vendor
Business Requirement	Responsible for scope and direction of the overall automation Responsible design standards, practices and principles	Informed	Maintain the list of processes that have automation potential Perform the assessment to prioritize the process that can be automated Participate in discovery sessions Provides Subject Matter Expertise (SME)	Participate in the discovery sessions Sign-off on the process that will be automated	Participate in discovery sessions Develop Process Definition Document (PDD)
Program Setup and Governance	Establish governance Evaluate ROI Manage resource allocation	Informed	Informed	Informed	Informed
Platform Administration and Operations	Maintains the solution Responds to incidents. Triages and prioritizes Validates the implementation for process, legal and security compliance Managed bot allocation and schedule	Deploys Robots to dev, test and production environments Provide access to the systems that are part of automation Administers users and access to dev, test production environments. Performs periodic review of the platform for security and performance	Manages exception processing workload Originates incidents Initiates business continuityactivities during bot downtime/issues	Act as the project manager/coordinator	Provides guidance on platform configuration
Robot Development	Consulted	Provides access to vendor Shadows vendor during development	Acts as the Product Owner Manages backlog of processes Performs testing	Acts as the project manager/coordinator	Develops new Robots
Process Changes	Consulted	Consulted	Oversees process changes Plans and executes the staff role revisions Defines workload redistribution	Defines and manages the change Documents the change Validates process changes	Recommends process changes
Training	Consulted	Supplies candidate students	Supplies candidate students	Supplies candidate students	Provides training on the tool and knowledge transfer
Security	Consulted	Enforces/validates security policies around data and access Implements secure coding practices	Provides input	Provides input	Implements platform security, secure credential storage and access management
Contract Management	Measures if the goals (ROI) of the automation are achieved	Owns the contract and software subscription	Owns day to day use and SLA monitoring	Informed	Accountable
Configuration Management	Informed	Approves production deployment of configuration updates	Informed	Informed	Provides development services for major updates. Owns production deployment of configuration updates
Upgrade Management	Informed	Implements platform upgrades	Tests changes and upgrades Understands new product features	Informed. Understand new product features	Provides upgrade guidance.

Automation Continuum



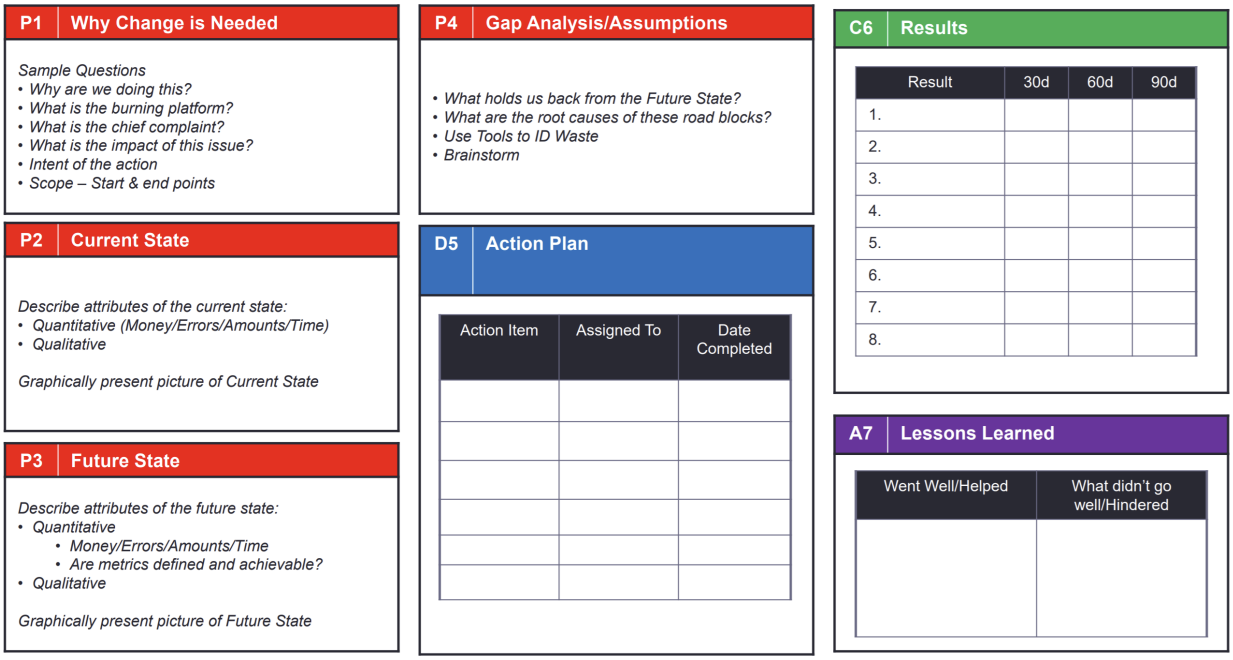
Graphic Source: Gartner

Use case selection and assessment

To successfully initiate an Intelligent Automation project, business teams and technical architects must collaborate through a structured discovery phase:

- **Process Identification and Analysis:** Business teams are responsible for identifying manual processes suitable for automation. This includes conducting a detailed time study for every sub-task to establish a baseline for current performance and to pinpoint bottlenecks that automation can resolve.
- **Architectural Consultation:** Business leads meet with an Intelligent Automation Architect to evaluate the technical feasibility of the use case. During these sessions, teams determine the **Level of Effort (LOE)** for development and the projected **Return on Investment (ROI)** to ensure the project aligns with organizational goals.
- **Role Designation:** To ensure accountability, the business team must appoint a dedicated **Automation Point of Contact (POC)** for daily or weekly coordination, a **Business Process Owner** to approve workflow changes, and an **Automation Manager** to oversee the project's lifecycle and resource allocation.

Business Case Planning Template:



P1 Why Change is Needed

Sample Questions
- *Why are we doing this?*
- *What is the burning platform?*
- *What is the chief complaint?*
- *What is the impact of this issue?*
- *Intent of the action*
- *Scope – Start & end points*

P2 Current State

Describe attributes of the current state:
- *Quantitative (Money/Errors/Amounts/Time)*
- *Qualitative*

Graphically present picture of Current State

P3 Future State

Describe attributes of the future state:
- *Quantitative*
  - *Money/Errors/Amounts/Time*
  - *Are metrics defined and achievable?*
- *Qualitative*

Graphically present picture of Future State

P4 Gap Analysis/Assumptions

- *What holds us back from the Future State?*
- *What are the root causes of these road blocks?*
- *Use Tools to ID Waste*
- *Brainstorm*

D5 Action Plan

Action Item	Assigned To	Date Completed

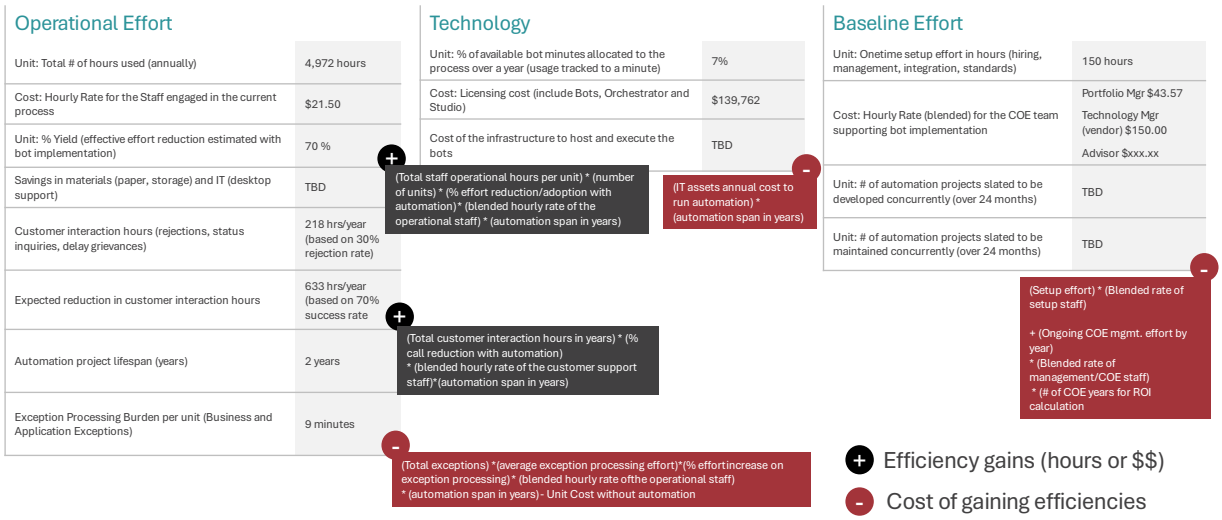
C6 Results

Result	30d	60d	90d
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

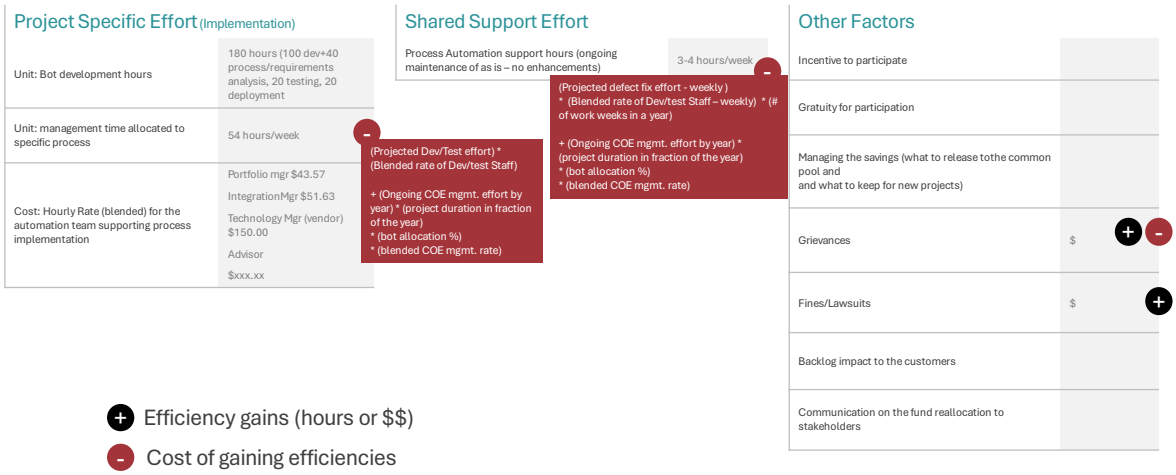
A7 Lessons Learned

Went Well/Helped	What didn't go well/Hindered

Detailed ROI Modeling. Example Part 1.



Detailed ROI Modeling. Example Part 2.



Use case Executive Team approvals

Concept

To secure executive approvals, business teams must develop and present a concise four-slide **Concept Pitch**. This "elevator-style" presentation is limited to 5–10 minutes, focusing on high-level value and feasibility to obtain an immediate "green light" or specific feedback for refinement.

The presentation structure is strictly defined as follows:

- **Project Identity** – Clearly identifies the project name and the core leadership team, including the Presenter, Business Process Owner, and Automation Point of Contact.
- **Use Case & Metrics** – Utilizes a four-quadrant layout (Background, Situation, Assumptions, and Recommendations). This slide must also display critical time-study data, including the number of positions involved, monthly transaction volumes, projected personnel savings, and the projected automation success rate.
- **Current State Process** – Provides a visual data flow diagram illustrating the existing manual tasks and processes.
- **Proposed Future State** – Displays a conceptual diagram of the automated workflow, highlighting how the technology solution will transform the process.

[LINK to Concept Presentation Template]

Execute Commit

This phase involves a comprehensive presentation that expands on the initial concept to secure final authorization for development. This expanded deck retains the original four slides but incorporates detailed operational data and a formal execution checklist.

The Execute Commit presentation adds critical details to move from a conceptual "green light" to active implementation:

- **Stakeholder Mapping**: Identification of specific technology and business contacts responsible for delivery.
- **Technical Specifications**: A deep dive into the specific tasks being automated and the precise Level of Effort (LOE) required from all participating teams.
- **Operational Checklist**: Verification of software licensing requirements, testing protocols, and staff training schedules.
- **Governance & Approvals**: Formal documentation of stakeholder notifications and necessary Human Resources (HR) approvals, particularly if the automation significantly alters employee roles, workloads, or classifications.

Once the Executive Team approves this detailed proposal, the project officially transitions into the build phase.

[LINK to Execute Presentation Template]

Readiness Review

A Readiness Review presentation is the final mandatory checkpoint conducted after the "Execute Commit" phase and before an automation's "Go-Live" date. The primary objective is to verify that the automation is technically sound, the business is prepared for the transition, and all governance guardrails are in place to prevent operational disruption.

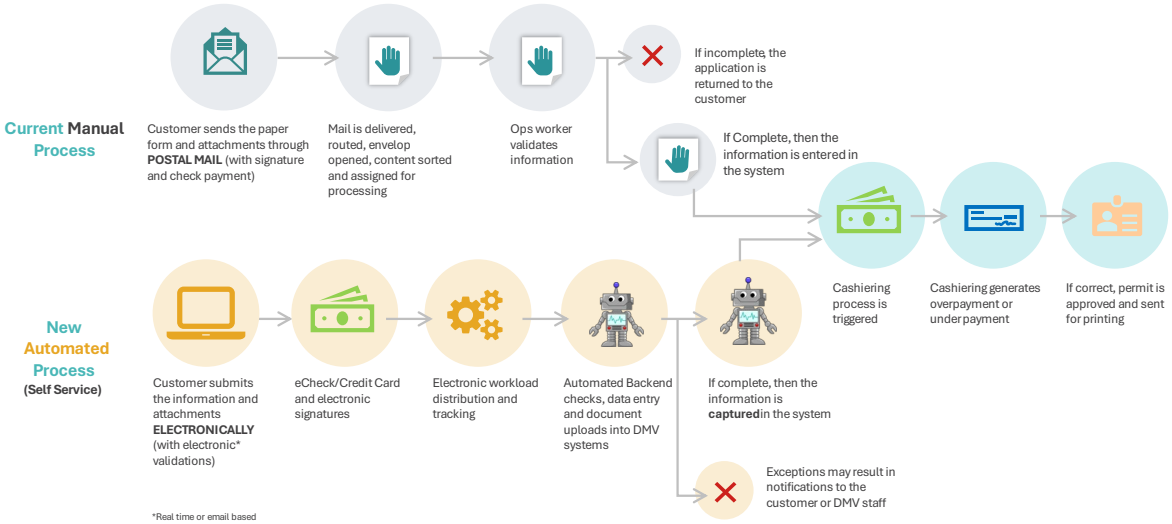
In addition to pages from execute commit, a readiness review focuses on the following:

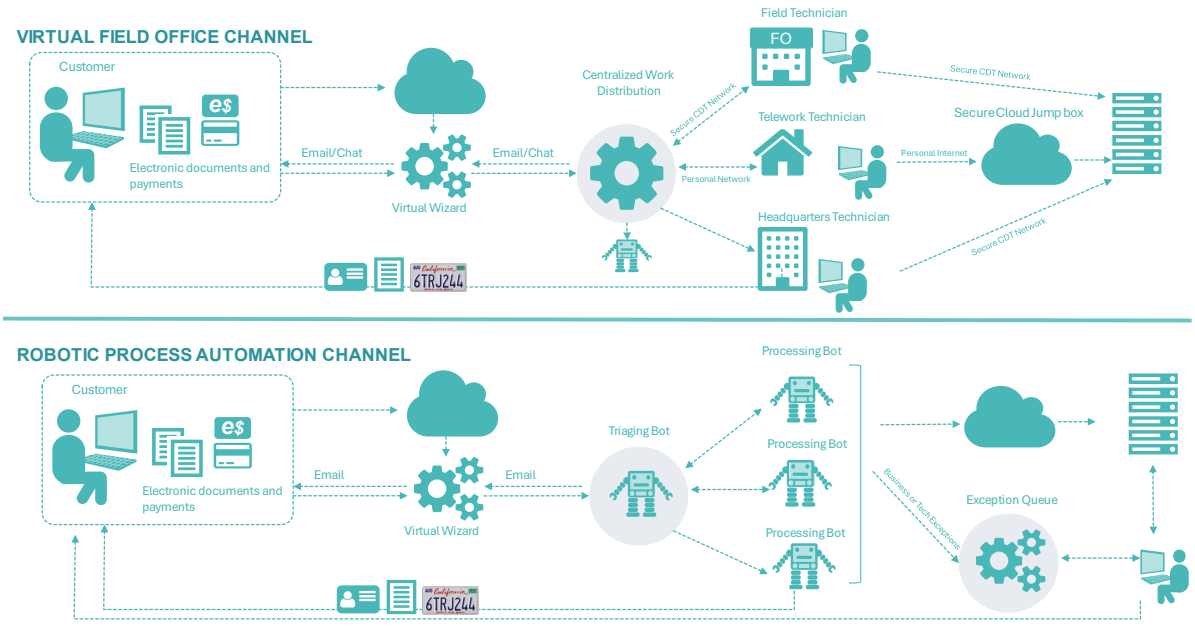
- **Technical Validation**: Provides acknowledgement of successful User Acceptance Testing (UAT) and confirms that monitoring dashboards are active for real-time observability.
- **Deployment Logistics**: Verifies that production environment resources are provisioned and that software licenses are active.
- **Business Continuity**: Outlines the incident response "runbook," including manual fallback procedures and support contact lists.
- **Workforce Readiness**: Confirms that impacted staff have completed training and that updated Standard Operating Procedures (SOPs) are published.
- **Security & Compliance**: Provides final sign-off from IT Security, ensuring data privacy and Role-Based Access Control (RBAC) are enforced.

The readiness review concludes with a **"Go/No-Go" decision**. Approval grants the team the formal authority to deploy, while any unresolved issues require a documented mitigation plan.

[LINK to Readiness Review Presentation Template]

Transforming a manual process with Automation





Operations Management

- ***Operations and Maintenance*** – In the early stages of an Intelligent Automation program, operations and maintenance are typically reactive. Because the low volume of pilot automations does not yet justify the overhead of active monitoring, resources are better invested in development to maximize initial returns. During this phase, automations often run until a failure occurs, at which point staff perform ad hoc mitigation. As a program scales to 10 or more automations, program must implement formal monitoring and maintenance frameworks to manage increased throughput and operational risk. These processes should scale proportionately with the complexity of the digital workforce. As Intelligent Automation program transition from pilot phases to enterprise-scale environments, the operational focus shifts from ad-hoc support to a centralized, platform-driven model. The Intelligent Automation Center of Excellence must prioritize migrating most of the digital workforce to a unified enterprise platform. This centralized approach ensures greater oversight, security, and resource optimization across the organization. As the portfolio grows, proactive communication becomes the primary safeguard against operational downtime. The Center of Excellence (CoE) must maintain continuous engagement with business units to forecast impending system updates or process shifts. To manage these evolutions, the program utilizes a formalized change management processes for submission, approval, and execution of use cases. This structured lifecycle ensures that as the program scales, it remains agile enough to adapt to environmental changes without compromising the stability of mission-critical services.
- ***Change Management*** – Business process evolve overtime, and any successfully automation program must follow a formalized Change Request procedure to maintain automation integrity and compliance. This typically begins with a request submitted through a centralized Service Management Portal, ensuring all modifications are tracked and audited. Before any technical execution, the proposed change must receive formal sign-off from all relevant stakeholders. If the modification requires updates to the automation's underlying code, the team must update the technical and functional specifications to reflect the new requirements, secure stakeholder approval on the amended PDD to ensure alignment between

business needs and technical delivery and ensure the updated PDD is archived within the Intelligent Automation Center of Excellence (CoE) repository for audit readiness. This structured approach prevents "scope creep" and ensures that every code change is validated against the original business objectives and current security standards.

- ***Automation Failures*** – Maintaining a stable automation catalog requires proactive environment management to ensure failures remain rare. Most disruptions stem from changes in production systems—such as software patches, UI updates, or modified credential requirements—rather than the automation logic itself. To mitigate these risks, the Intelligent Automation Center of Excellence must maintain a comprehensive registry for every automation, documenting all required software versions, system interfaces, and credential types. This record must be established at deployment and updated during every maintenance cycle. The CoE should maintain a continuous feedback loop with business units and IT departments to identify impending system changes, and by tracking updates before they occur, development teams can adjust bot configurations in advance, preventing any loss of functionality or service delivery.
- ***License Management*** – Each department's Intelligent Automation program will consist of different set of automations. Some will focus only on web automations, others may include a variety of use cases that rely on bulk data intake, document data extraction, robotic process automation, workload management, etc. Software licensing structures vary by provider but generally revolve around run-time capacity, number of use cases, and the number of transactions processed. In a typically RPA model, one robot license supports up to 24 hours of execution daily, seven days a week. For instance, a program requiring 48 total hours of daily run-time across multiple automations would need at least two licenses. Costs are further influenced by the type of automation chosen. To control costs, departments should maximize license utilization through rigorous planning. State of California procurement cycles often involve long lead times, which can create gaps between when an automation is ready and when capacity is available for deployment. The Intelligent Automation COE must forecast license requirements up to a year in advance. While it is best to avoid purchasing licenses before they are needed, precise forecasting ensures that automation deployments align with procurement timeframes for a seamless delivery.

- ***Lifecycle Management*** - To ensure security and scalability, enterprise level automation platforms must utilize distinct environments for development, testing, acceptance, and production. Lifecycle management facilitates this by providing a framework for the continuous testing and deployment of automations, robots and their dependencies across the software development life cycle. This structured approach allows automations to transition seamlessly through organizational stages before production release. Enforcing Role-Based Access Control is essential for maintaining compliance and safeguarding mission-critical services as automation complexity grows.
- ***Code Sharing*** - Mature automation programs can accelerate scaling by creating reusable automation components across business units that utilize the same core applications. By establishing a centralized library of common actions, such as standard login sequences, developers can improve resiliency and speed up the build process. As development demands increase, technical teams should implement code-sharing techniques to expedite delivery. This is best achieved by storing snippets in a secure, shared environment. While most enterprise automation platforms offer built-in asset libraries for this purpose, internal code repositories can serve as a functional alternative for code storage and accessibility.
- ***Automation Scheduling*** – As the use cases become more complex, and more and more processes are deployed using the Intelligent Automation solutions, it is required to have a designated team member from within the automation team to work directly with the business teams to decide how new automations will be scheduled on existing licensing constraints. Unattended automation can be scheduled to run at a specific time of the day, specific days, or in response to an external trigger. The assigned individual(s) will be tasked with ensuring automation schedules are being followed and automations are executing as designed.

Workforce Planning

- ***Employee Engagement*** – [To be completed]

- ***Workforce Planning*** – [To be complete]

- ***Upskilling Employees Affected by automations*** – As Automation programs expand and are used in operations, employee responsibilities may be alleviated. [To be complete]

Executive Reporting / Business Value

- [To be completed]
- [To be completed]

APPENDIX / REFERENCES

[To be complete]

CONTRIBUTORS

[To be complete]