

Automation at the Heart of Healthcare Operations

A turnkey operating model that shifts cost, risk, and accountability.



lgi healthcare
solutions

Beyond Platforms: The automation model that stands the test of time

Healthcare leaders do not lack automation proposals. What they lack is a finance-grade view of total cost, risk, and accountability once automation is live inside a complex, constantly changing environment.

Most automation business cases focus on licenses, implementation, and return on investment (ROI). In practice, platform-centric automation behaves like an open-ended commitment. Internal teams absorb ongoing build, test, break-fix, governance, and incident response work. Every electronic health record (EHR) upgrade, payer portal change, or user interface (UI) update creates unplanned effort. Accountability fragments across vendors, IT, and operations. Costs drift. Risk compounds.

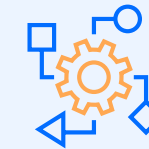
The real choice is not tools versus tools. It is between:

- A platform you must build, operate, and continuously repair, carrying internal cost, staffing dependency, and continuity risk.
- An Automation Agent-as-a-Service (AAaaS) model where LGI designs, builds, runs, and monitors virtual agents inside your environment as a managed service, converting that exposure into a predictable operating expense with clear boundaries, accountability, and outcomes.

Who this guide is for



Finance leaders who need a defensible, finance-grade view of total cost, risk transfer, and budget predictability for automation at scale.



Technology leaders who must decide whether to keep building and running automations internally or delegate that responsibility to a managed AAaaS vendor.



Operations leaders who care most about throughput, quality, staffing flexibility, and resilience in critical workflows.

This ebook helps leaders assess whether internal automation platforms still make financial sense — or whether an AAaaS model provides a more predictable and lower-risk path forward.



Automation Ownership Over Time: **Platform vs As-a-Service**

Healthcare executives are being asked to fund automation while protecting thin margins, managing chronic labor shortages, and reducing operational and security risk. Platform-centric automations deliver value, but for many organizations the business case breaks under four recurring patterns:

Financial risk: **CAPEX becomes hidden OPEX**

Initial licenses and implementation turn into ongoing infrastructure, consulting, and “mini projects” over three to five years. The fragmented spending looks like one-time investment but behaves like a continuous operational expense, without the predictability you need for budget planning.

Operational risk: **Hidden internal lift**

Vendor proposals understate the time required from IT, revenue cycle, patient access, and compliance teams to design, test, and maintain automations. Automations wired to screens and portals may fail when upstream systems change, forcing internal teams to rebuild scripts to restore baseline performance. The platform is technically in place but expensive to expand. Budget gets tied up keeping today’s automations stable while expansion stalls. That is operational debt.

The outcome: **Failure to scale**

These risks converge into a single result: the platform cannot reliably expand because it is too dependent on internal specialists, and too expensive to maintain. You are left with accumulated operational debt and constrained capacity.

What AAaaS changes: **The risk comparison**

Against this backdrop, here is how AAaaS reduces exposure over the next three to five years.

Risk type	Platform model	AAaaS model
Financial 	Fragmented CAPEX that behaves like OPEX; ongoing “mini projects” and consulting; cost curve is unclear	Single all-inclusive subscription with defined scope, including licenses, design, build, run, monitoring, and in-scope change handling; predictable annual cost
Operational 	Internal teams responsible for build, maintenance, and every change response; scarce specialists stretched thin; fragility limits expansion	LGI assumes the role of dedicated automation authority; your teams focus on strategic guardrails and approving changes; single accountable owner for performance and service levels

Bottom line

Instead of owning an automation layer and its accumulated operational debt, you own the outcomes and oversight while LGI owns the automation factory and its day-to-day risk. Automation behaves like a reliable operational capability instead of another platform your teams must own, staff, and defend.

The Foundation of a Finance-Grade Automation Business Case

Automation business cases fall apart in front of a CFO when inputs are vague. Volumes get estimated from memory. Full-time equivalent effort is guessed. Risk is described in generic bullets instead of being tied to real incidents and exposure. Leaders rarely reject automation because they dislike the idea. They reject assumptions they cannot defend.

A credible automation business case starts with a small set of core data points that apply regardless of the model — whether you run a platform internally or shift to an as-a-service approach:

Operational baseline: **What work are you really doing?**

Start with how work actually moves today in your highest-impact areas, typically revenue cycle, patient access, and key back-office workflows. Capture performance indicators tied to the workflows that materially affect cash, throughput, or staffing.

Financial baseline: **What does that work really cost?**

Translate the operational view into a finance view using labor costs, including outsourced services, temporary staffing, and existing tools and support fees.

Risk and compliance baseline: **Where are you exposed today?**

Executives evaluate automation on cost and risk. Build a simple baseline across operational risk, process and quality risk, and compliance and audit risk, based on what has actually happened in the last one to two years. The goal is to gain visibility into where risk sits today and how each operating model changes it.

Budget and project landscape: **What will this investment compete with?**

Even a strong automation case competes for funding and the same constrained teams. Position AAaaS as a defined OPEX subscription versus a platform approach that often presents as CAPEX plus internal program cost.

Together, these baselines allow you to clearly quantify cost and throughput impact, surface risk in financial terms, and compare platform-based automation with an AAaaS model in a consistent, finance-grade way.



Understanding Automation Models

To compare automation options fairly requires a clear view of the operating models being evaluated — including where responsibility, cost, and risk sit over time.

Status quo: Manual work and patchwork tools

- **What it looks like:** repetitive, rules-based work handled manually with local scripts, macros, point tools, and workarounds, plus ongoing support from IT and analytics to keep queues moving.
- **Where the money goes:** labor dominates, including overtime, temporary staff, and outsourcing when backlogs spike, with fragmented vendor spend across niche tools and services.
- **Risks and constraints:** costs rise with volume and wage pressure, processes remain fragile, and resilience is limited when systems, payers, or staffing change.

CAPEX automation platform: Tools plus an internal program

- **What it looks like:** buy a platform, then stand up an internal automation team to design, build, and maintain automations as the business submits use cases.
- **Where the money goes:** CAPEX for licenses and implementation, plus ongoing OPEX for the IT and internal automation team, infrastructure, specialized talent, consulting, and remediation when systems change.
- **Risks and constraints:** a second cost layer on top of core systems, dependence on scarce specialists, fragility to EHR and UI changes that trigger “fix it now” work, and fragmented accountability when something breaks. The specific cost, risk, and fragility issues are detailed earlier in this guide.

LGI Automation Agent-as-a-Service: Automation as a managed service

LGI Automation Agent is available as a service, not as a one-time CAPEX platform purchase. You fund a single OPEX subscription that covers licenses, the automation stack deployed inside your environment, the virtual agents that execute work, and the service required to keep them running.

- **What it looks like:** LGI designs, builds, runs, and monitors virtual agents for specific workflows as a turnkey service, with LGI serving as the automation center of excellence alongside your teams.
- **Where the money goes:** one all-inclusive subscription covering the LGI licenses, the agents, and service for design, build, run, monitoring, and in-scope change handling, with incremental spend only for work explicitly outside the agreed scope.
- **Risks and constraints:** reduced backlog and firefighting after payer or EHR changes, minimal internal lift for IT, with execution and audit staying within your perimeter.



The difference between models is not the automation itself, but where cost, risk, and accountability live over time.

Consideration	Platform	AAaaS
Funding & cost structure	Upfront platform investment plus ongoing internal program costs that behave like operating expense over time	Single subscription structured as operating expense
Cost predictability	Hard to forecast as automation scales and systems change	High predictability with defined scope and service obligations
Internal effort & ownership	Internal teams design, build, monitor, and maintain automations	LGI designs, operates, monitors, and maintains automation agents
Change handling	System and UI changes trigger internal remediation projects	Normal system and UI changes handled as part of the service
Scalability & resilience	Limited by internal capacity and sensitivity to staffing or priority shifts	Designed to scale with greater continuity despite system or staffing change
Risk & accountability	Risk and operational burden remain internal as automation footprint grows	Risk concentrated within a managed service with clear accountability
What leadership ultimately owns	The platform, the team, and the ongoing operational burden	Outcomes, oversight, and strategic direction

Ownership and cost define the model, but resilience is determined by how automation responds to system change.

Automation in a **Dynamic System Environment**

Automation does not operate in isolation. In healthcare, it spans clinical systems, payer portals, patient access workflows, and financial platforms — all of which evolve continuously.

As these environments change, automation is affected in ways that are rarely visible at deployment. Interfaces shift, rules evolve, and dependencies change, often without notice. While these changes may not appear on implementation plans, they directly influence automation performance and the effort required to keep work moving.



Over time, system change introduces:

- **New points of exposure**
Screens, fields, and validation rules evolve, creating conditions automation must respond to.
- **Operational friction**
Breaks and exceptions require investigation, testing, and remediation — frequently under time pressure.
- **Hidden effort**
Monitoring and repair work accumulate quietly, drawing on specialized skills and competing with other priorities.
- **Uneven reliability**
Automation performance can vary as complexity increases and change accelerates.

How an automation model responds to these conditions is one of the clearest indicators of long-term sustainability.

In platform-based approaches, adaptation to change is typically absorbed by internal teams through ongoing monitoring, testing, and repair. Over time, this effort compounds and limits scalability.

By contrast, models designed to anticipate change treat adaptation as a normal operating condition, maintaining performance as systems evolve rather than reacting after issues surface.

Understanding this difference sets the stage for examining where automation exposure exists and how it shapes outcomes over time.

Where Automation Exposure Exists

Rather than documenting every system detail, executives benefit from understanding **where automation is most exposed to change and which factors influence long-term reliability**.

Key areas of exposure include:

- **Systems involved**
The number and type of applications, portals, or interfaces a workflow depends on — including EHRs, payer portals, clearinghouses, and third-party tools.
- **Touchpoints and handoffs**
Where automation interacts with user interfaces, data fields, rules engines, or external validations that may change without notice.
- **Change frequency**
How often those systems or interfaces are updated, redesigned, or governed by external parties outside the organization's control, including changing regulatory environments.
- **Operational sensitivity**
The degree to which delays, errors, or interruptions in this workflow create downstream impact for patients, staff, or revenue.
- **Current mitigation effort**
The amount of monitoring, manual checking, or rework required today to keep the workflow moving when conditions change.

Over time, these factors influence how automation performs:

- **Reliability under change**
Workflows that rely on frequently changing systems place sustained pressure on automation models not designed to absorb variability.
- **Accumulated operational effort**
Monitoring, testing, and repair work can grow quietly, eroding expected efficiency gains.
- **Scalability constraints**
Models dependent on internal specialists tend to scale unevenly as exposure increases.
- **Long-term sustainability**
The ability to maintain performance through change matters more than initial deployment speed.

Automation as a Service: **Shifting Cost, Risk, and Accountability**

Automation-as-a-Service reframes automation from a platform investment into a managed operating capability.

The model does not change the work that needs to be done — it changes who owns the responsibility for getting it done, and who carries the risk when conditions change.

Under an AAaaS model, automation is delivered as a service rather than a platform your teams must build, operate, and continually repair.

The same workflows, volumes, and system realities remain in place, but once deployed accountability shifts from internal teams to a defined service model with clear boundaries, obligations, and oversight.



How **Accountability** is Delivered

Automation-as-a-Service is not a tool purchase. It is a managed operating model with clearly defined responsibility for delivery, continuity, and change.

- **Licenses, design and build**

With all licenses included on the subscription, LGI then designs and builds virtual agents for agreed workflows, aligned to your processes, controls, and operational guardrails.

- **Run and monitoring**

LGI operates agents day-to-day, monitors performance, and manages incidents through defined escalation paths.

- **In-scope change handling**

For covered workflows, normal system and interface changes are handled as part of the service — not treated as new projects.

- **Service governance**

Regular governance ensures priorities, scope, and performance expectations remain aligned, with clear roles across LGI, IT, security, and operations.

All of this runs on an LGI-owned automation stack deployed inside your environment. Execution and audit remain within your existing security and access model.

Financial Structure and Operating Impact

Under an AAaaS model, automation is funded as a single, predictable operating expense rather than a collection of platform, staffing, and remediation costs that accumulate over time. The subscription covers the licenses, orchestration, and virtual agents for defined workflows and volumes, including normal system and interface changes within scope. Internal effort is intentionally limited to governance, prioritization, and approvals — not day-to-day operation or repair.

The Impact of This Model is Felt Across the Organization:

- **IT** avoids standing up and maintaining a separate automation platform, reducing ongoing build, monitoring, and repair work as systems evolve.
- **Security and compliance** keep execution, logging, and audit activity inside the existing environment.
- **Operations** experience less disruption when EHR screens or payer portals change, because maintaining automation continuity is part of the service.
- **Finance** gains a clearer, more predictable cost profile, replacing layered capital investment and incremental remediation with a single operating model aligned to outcomes.



What Accountability Looks Like in Practice

Shifting accountability is not theoretical. It changes how automation is supported once it is live — especially when systems change, priorities shift, or issues arise.

- **Day-to-day operation**

Automation is monitored and managed as a production service, not an internal side responsibility.

- **Issue response and resolution**

When errors, exceptions, or system changes occur, response and remediation are part of the service obligation — not an ad hoc internal effort.

- **Continuity through change**

EHR upgrades, payer portal changes, and interface updates no longer trigger emergency internal projects; maintaining continuity is built into the model.

- **Clear ownership**

Your teams retain oversight and decision-making authority, while LGI owns execution, reliability, and follow-through.

This shift in accountability is what allows automation to behave like a stable operating capability rather than another platform your teams must continuously manage.

Where Organizations see **Early Value from Automation-as-a-Service**

Organizations that succeed with AAaaS do not start everywhere at once. They focus first on workflows that combine measurable impact, operational friction, and ongoing exposure to system change — areas where a managed model delivers immediate value and reduces internal strain.

First-wave virtual agents tend to share a few common characteristics:

- They touch high-volume, repeatable work tied directly to cash flow or service levels
- They rely on external systems or portals that change frequently
- They consume disproportionate staff time through manual checking and follow-up
- They create visible operational relief essentially immediately, with ROI typically within six to twelve months

Common first-wave automation categories include:

- Claim adjustments
- Insurance verification
- Denied claims processing
- Materials management
- Claim status checking

From Early Wins to Sustainable Value

The value of these early automation efforts is not just faster deployment. It is continuity. These workflows continue to perform as systems change, volumes fluctuate, and priorities shift — without becoming another operational burden for internal teams.

That reliability is what allows organizations to move from isolated automation wins to a sustainable operating capability.



Moving from Evaluation to Action

The decision is no longer whether automation can deliver value, but which operating model you are prepared to own over time — and how much cost, risk, and operational responsibility you want to carry internally.

Many organizations choose to move forward by validating AAaaS against a small number of high-impact workflows, using their own data and systems to confirm fit, value, and operating alignment. This approach allows leadership teams to see how the model performs in practice — without committing to a large platform investment or long-term program upfront.

Next step

Connect with LGI to discuss priorities, scope, and options for validating AAaaS within your organization.

LGI can support this evaluation through a focused, low-risk engagement that allows organizations to experience LGI Automation Agent-as-a-Service in their own environment before making longer-term decisions.

lgiautomationagent.com