# RPA Readiness Assessment

Scoring processes for automation potential, control risk and maintainability before any bot is built.

Nov 10, 2026 · @Vijay Srinivas Kothapalli

## Purpose

Robotic process automation can save hours of routine work, but a poorly chosen process produces a fragile bot, hidden control gaps and disappointed managers. This assessment helps you decide, before any build, whether a process is worth automating, needs fixing first, or should not be automated at all.

It gives a score across five areas and a clear decision, so the choice is made on evidence rather than enthusiasm.

## When to use it

Use the assessment before any of these:

- A proposal to automate a process from a team, a vendor or a consultant.
- A decision to buy or license automation tools.
- A plan to replace manual work during a headcount reduction or a growth push.

Repeat it when a process changes materially, such as a new system, a new supplier or a change in the rules it follows.

## The assessment at a glance

1. **Suitability.** Is the process rule-based, digital and repeatable?
2. **Volume and value.** Is there enough work to justify the effort?
3. **Stability and rules.** Do the steps and the rules stay the same for long enough?
4. **Controls and risk.** What happens if the bot makes a mistake, and who checks it?
5. **Data and system access.** Can the bot reach what it needs, safely and without shared logins?

Each area is scored from 1 (poor) to 5 (strong). The total decides the outcome.

## Part 1: Suitability

Score 5 when the work is entirely digital, follows fixed rules and needs no judgement.

| Score | What it looks like |
|---|---|
| 5 | Data arrives in a known format, each step is a fixed rule, and no reading of documents or free text is needed |
| 3 | Mostly rule-based, with some documents to read or some judgement on exceptions |
| 1 | Relies on phone calls, handwritten notes, or a person deciding case by case |

Any process that needs a human to interpret meaning, such as a complaint or an unusual contract, is a poor candidate for a first bot.

## Part 2: Volume and value

Measure how often the process runs and how long each run takes by hand. Then estimate the annual hours it consumes.

**Worked example.** A payables task runs 400 times a month, takes 6 minutes by hand, and needs a 1 in 20 rework rate. Annual manual effort is about 400 × 12 × 6 minutes, or 48 hours a month less rework. Compare this with the total cost of build, licences, support and the time to maintain the bot over three years. Automation should pay back within a sensible period, usually under 18 months, after allowing for maintenance.

Score 5 for high volume with a clear payback. Score 1 for work that runs a few times a year.

## Part 3: Stability and rules

A bot breaks when the process changes. Check how often the steps, screens, forms and business rules change.

- Score 5: the process has run the same way for over a year, and changes are announced in advance.
- Score 3: changes happen a few times a year, and the team is told about them.

- Score 1: screens, forms or rules change without notice, or each team does the task differently.

Where the process varies by team, standardise it first. Automating several versions of the same task multiplies the maintenance.

## Part 4: Controls and risk

Ask what the process protects. Payments, approvals, customer data changes and regulatory filings need controls that a bot must respect, not bypass.

- Is there a segregation of duties today, and does the bot preserve it?
- Can every bot action be logged and traced to a named request?
- Are exceptions escalated to a person, with a clear owner and time limit?
- What is the worst outcome of a wrong run, and how fast would it be found?

Score 5 when the controls are clear, logged and unchanged by automation. Score 1 when the process has weak controls today, because automation will scale those weaknesses.

## Part 5: Data and system access

A bot needs access to systems, and that access is a security risk in its own right.

- Score 5: the bot uses its own named service account, with the least access needed, and credentials are stored in a managed vault.
- Score 3: access is granted, but credentials are shared or reviewed only once a year.
- Score 1: the bot would use a person's login, or needs administrator rights.

Record which systems the bot will touch, what data it reads and writes, and where logs are kept. Check that the process does not move personal data into a place it should not go.

## Scoring and the decision

Add the five scores. The total ranges from 5 to 25.

| Total | Decision | What happens next |
|---|---|---|
| 20 to 25 | Go | Proceed to a controlled pilot on the process |

| Total | Decision | What happens next |
|---|---|---|
| 14 to 19 | Rework first | Standardise the process, tighten controls or reduce variation, then reassess |
| 5 to 13 | Do not automate | Keep the process manual, or redesign it fundamentally before considering automation |

Any area scored 1 blocks a Go decision until it is addressed, even if the total is high. A bot with weak controls or shared logins should not go live, whatever its payback.

## Warning signs to watch for

- The business case depends on a saving nobody has measured.
- The team describes the process differently from how it is actually done.
- The process has many exceptions, and the exception rate is not known.
- The vendor sells a bot before anyone has examined the process.
- The automation is expected to fix a broken process.
- Staff are told the bot will replace roles before the design is agreed.

Any one of these is a reason to pause and reassess.

## From assessment to a controlled pilot

1. **Document the process as it runs.** Walk it with the people who do it, and record each step and exception.
2. **Fix the obvious.** Remove duplicate steps and agree one standard way of working.
3. **Agree the controls.** Write down the approvals, logs and exception rules the bot must keep.
4. **Build in a test environment.** Use test data and a named service account.
5. **Pilot with a limit.** Run the bot alongside people for four to six weeks, with every output checked.
6. **Review and decide.** Compare results, errors and hours saved against the business case, then approve full use or stop.

## Governance after go-live

- **Name an owner** for each bot, in the business and in IT, with a backup for each.
- **Keep a register** of every bot: purpose, process owner, systems accessed, credentials, last review and the controls it relies on.
- **Review access** to bot accounts every quarter.
- **Monitor** run counts, failures and exceptions. Set an alert for unusual volumes.
- **Re-run the assessment** when the process, the system or the rules change, and at least once a year.
- **Plan for the bot to stop.** Know the manual fallback, and keep it current.

## About CRCO LLP

CRCO LLP is a Hyderabad-based advisory firm working with businesses on process improvement, business process reengineering, robotic process automation, outsourcing and data protection. We run readiness assessments, redesign processes before automation, and help teams set up the controls that keep bots safe.

**Book a consultation:** visit the Contact page on our website, or write to us through the enquiry form.

*This framework provides general guidance only. It is not technical or legal advice. Each automation should be designed and tested for your own systems and obligations.*