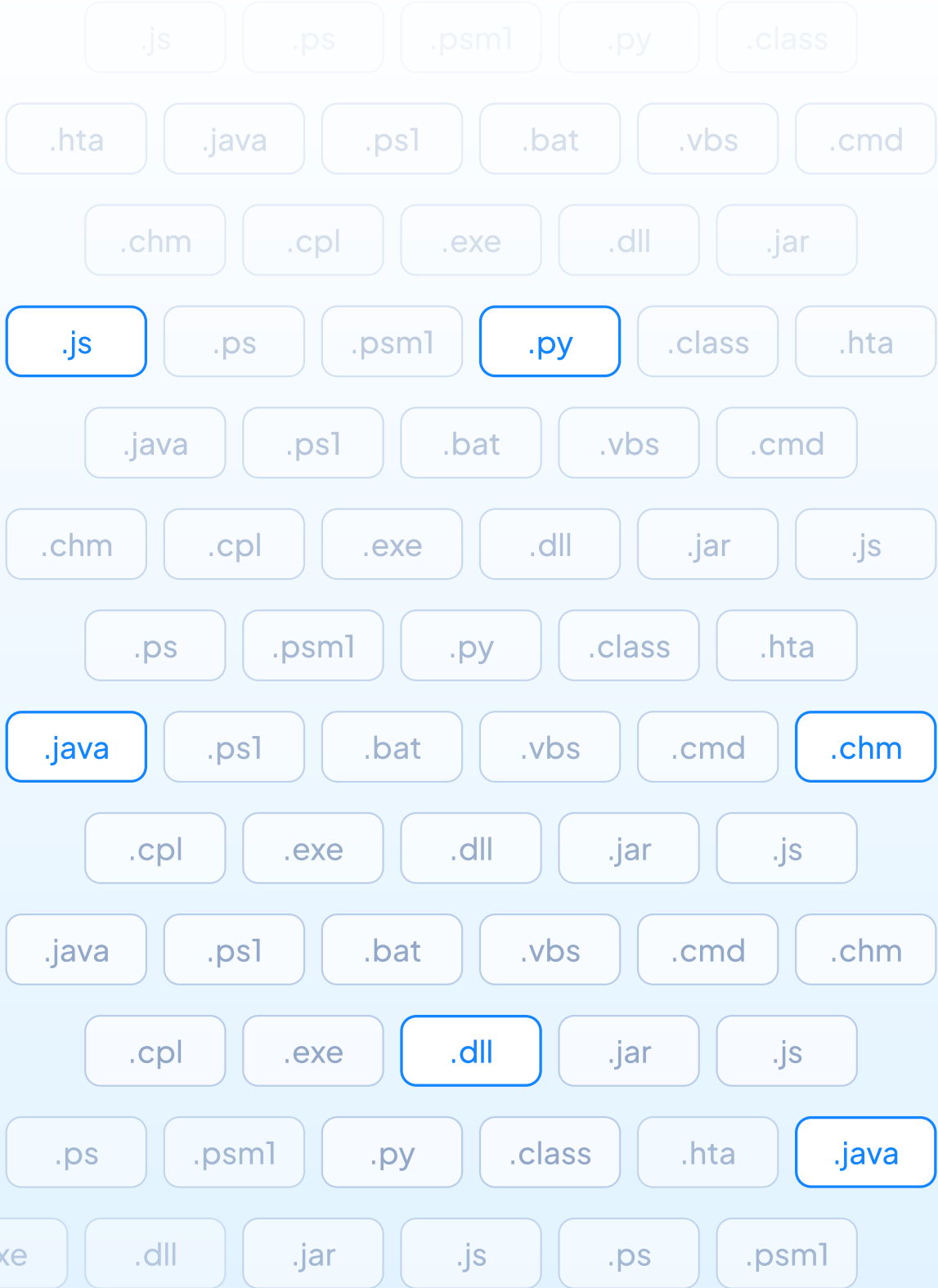




Application Control Replacement Readiness Checklist

Keep the control. Change the operating model. Know what to preserve, what to improve, and what to validate before you move.



Use this checklist to assess your current application control program and identify what to preserve, what to improve, and what to validate before moving to a new solution. It helps you separate what you already know from what requires internal discovery or technical validation, so you can define how your organization will govern and maintain trust at scale. An unchecked item isn't necessarily a blocker, it's a question to resolve before you make enforcement decisions.

Current operating picture

☐

We can quantify or describe the administrative, endpoint, infrastructure, and support burden of the current environment.

☐

We know which concerns are widespread and which are limited to particular teams, operating systems, environments, or workflows.

☐

We understand where certificate changes, installer and updater chains, MSI handoffs, scripts, developer activity, or recurring exceptions create administrative work.

☐

We have identified the security outcomes a replacement must preserve and the operating conditions it should be evaluated against.

Requirements and governance

Define what a new solution must support: the applications and workflows your business depends on, who owns trust and risk decisions, which endpoints and environments are in scope, and which integrations your security and IT operations require.

- ☐ We know which applications, software sources, users, systems, and workflows are business-critical.
- ☐ We know who owns trust, exception, policy, risk, and enforcement decisions.
- ☐ We have identified required endpoint, server, workload, legacy, and developer personas, along with proposed VDI, OT, and constrained-environment deployments that require validation.
- ☐ We have defined required integrations, reporting, authentication, logging, deployment, and data-residency capabilities.

Policy and workflow readiness

Your existing policies hold years of valuable decisions, along with rules that may no longer serve a purpose. Separate current security requirements from stale or product-specific configuration, understand how software enters your environment, and define the exception and approval experience you want going forward.

- ☐ We can distinguish current security requirements from stale or product-specific configuration.
- ☐ We understand how approved applications, updates, installers, updater chains, MSI handoffs, scripts, and developer builds enter the environment.
- ☐ We understand which future software-delivery workflows may use Trusted Installer and that software already present remains subject to standard allowlisting.
- ☐ We know where permanent local exceptions or broadly ignored paths have created drift or blind spots.
- ☐ We have defined the exception and approval experience we want to operate going forward.

Transition readiness

Plan a staged transition that moves forward on evidence, not elapsed time. Run your new solution alongside your existing environment under an approved coexistence plan, validate enforcement with a representative population, and confirm rollback, retention, and decommissioning requirements before expanding.

- ☐ We have identified a representative initial deployment population and the applications and workflows it must exercise.
- ☐ We have defined success measures for endpoint impact, policy quality, application coverage, administrative effort, support impact, and enforcement confidence.
- ☐ We understand coexistence requirements, necessary changes to the current solution, rollback, data retention, agent removal, and infrastructure decommissioning.
- ☐ We have identified who is responsible for each transition stage on our team and at Airlock Digital, along with the criteria for completing each stage.

Next Steps

Go deeper. For more detail on what to assess, preserve, and improve before moving to Airlock Digital, download the [Replacement Readiness Guide](#).

Talk it through. Bring your current pain points, critical workflows, platform requirements, and readiness gaps to a [replacement-readiness discussion](#) with Airlock Digital. Together, we'll define what a successful transition should improve before deployment begins.



About Airlock Digital

Built for complex, distributed environments, Airlock Digital gives security and IT teams visibility across their endpoints and the control to decide what belongs. Organizations define trust based on how their business actually operates, build policies around that definition, validate their impact before enforcement, and keep protection effective as their environment changes. Purpose-built workflows and deep endpoint expertise make preventative controls practical to deploy, enforce, and sustain at enterprise scale.