Island

Checklist

The technical evaluator's validation checklist

This gives your architecture and security teams a structured way to pressure-test Island against a single access workflow before any deeper evaluation. Work through it and you'll have a clear view of what's confirmed for that workflow and what still needs work.

Start with one workflow. Before anything else, choose the one access path you're validating:

- ☐ BYOD and unmanaged-device access
- ☐ Citrix / VDI offload
- ☐ VPN / RDP reduction
- ☐ SaaS and browser governance

The checklist

Check off each item you can confirm for the workflow you chose. Anything you can't check yet is an open question to resolve before you go further.

1. Workflow scope and baseline

Pin down the specifics of the workflow you selected, and capture the baseline friction or risk you want to improve so you have something to measure against later.

- ☐ User population and device pattern are defined
- ☐ Applications and client environments are listed
- ☐ Current access path is documented (browser, VDI, VPN, RDP)
- ☐ A business owner and a technical owner are named

2. Identity and device context

How people authenticate, and what changes across managed and unmanaged devices, shapes every policy decision that follows. Unmanaged and shared devices usually raise the hardest requirements, so look there first.

- ☐ Identity provider and SSO/MFA path are confirmed
- ☐ User groups and role mapping are defined
- ☐ Managed, unmanaged, shared, and non-standard devices are accounted for
- ☐ Device posture inputs and their policy effects are understood

3. Access and application boundary

The goal is least privilege for the workflow: the apps and environments it needs, and nothing broader. Be explicit about what's deliberately out of scope, and record the exception path.

- ☐ Required SaaS, web, private, and client environments are inventoried
- ☐ The entitlement and role model is defined
- ☐ Access to keep out of scope is identified
- ☐ Private-app and network dependencies are documented

4. Browser and data controls

This is the heart of the evaluation: what actually gets controlled inside the session. Decide which data actions you need to govern, and how policy should vary by context.

- ☐ Data actions to govern are listed (copy, paste, download, upload, print)
- ☐ Policy varies correctly by user, device, application, and data context
- ☐ Sensitive-data handling is defined where it applies
- ☐ Test cases and expected control behavior are written down

5. Access-path fit: network, VPN, and VDI

Look at what the workflow uses today, and be honest about what still needs it. Some work belongs on the network or a full desktop, and keeping the current path is a valid result.

- ☐ Current network, VPN, and RDP dependencies are mapped
- ☐ Sanctioned destinations and private-app needs are defined
- ☐ Parts that require full desktop delivery are identified
- ☐ Coexistence or offload boundary and a rollback path are agreed

6. Logging and evidence

Decide up front what Security, Risk, and Compliance need to be able to prove after the fact. If you can't yet say what you'd need to prove, that's a gap worth surfacing now.

- ☐ Required session, policy, and data-action events are defined
- ☐ Logging destination (SIEM or other) is confirmed
- ☐ Alerting, retention, and ownership are agreed
- ☐ Existing DLP and logging behavior is accounted for

7. Coexistence with your stack

Island is meant to run alongside what you already own, not replace it. Use neutral fit criteria, not a displacement score, and treat documenting where an existing control stays in place as a valid outcome.

- ☐ Fit against your incumbent browser and controls is assessed on neutral criteria
- ☐ Overlap and separation with identity, endpoint, DLP, SIEM, and SSE/ZTNA are documented
- ☐ Managed and unmanaged coverage is compared
- ☐ Any contract or ownership constraints are noted

8. Deployment and operations

A workflow isn't validated until you know how it runs day to day, and what happens if you need to back it out. Day-two gaps don't disqualify a workflow, but they do belong on the plan.

- ☐ Pilot scope and admin model are defined
- ☐ Configuration and change control are planned
- ☐ Support, monitoring, and help-desk impact are covered
- ☐ A rollback and escalation path exists

Make the call

Once you've worked through the workflow, the pattern points the way:

- Mostly checked, with only minor gaps: move to a technical validation plan.
- Checked on fit, but open questions on controls, logging, or operations: close those first.
- Key items unchecked, or an existing control clearly does the job: keep the current path for this workflow.

Whatever's left unchecked is your list of open questions to resolve before anyone invests further.

Next step

If the workflow is ready to progress, the next move is a technical conversation with the Island team.

Request a demo