Control Mapping Pack: Security + Compliance

A practical way for public sector teams to turn control requirements into browser policies with Island

REDLEIF

Island

Control Mapping Pack: Security + Compliance

> "Last-mile" controls are the guardrails enforced where work actually happens: inside the browser session.

Public sector security teams are often asked to tighten controls without slowing work to a crawl. That becomes especially hard when the "point of work" is a browser session that changes depending on who is accessing what, from where, and under which constraints.

This mapping pack is for public sector security and IT teams who are evaluating Island, rolling it out, or tightening existing Island policies. It helps you translate common control requirements into a baseline you can defend internally, then refine over time.

Use it when

- You need a conservative starting point for a new Island rollout.
- A high-risk workflow needs tighter controls (contractors, sensitive SaaS, privileged access).
- You are aligning Security, IT, and stakeholders on what will be enforced and why.

What you get (and what it is not)

This deliverable includes three components:

Control Mapping Worksheet

A simple worksheet that connects what you are protecting to the controls you want enforced at the point of work.

Example Policy Starter Set

Prebuilt "good defaults" you can use as a baseline, then tighten based on risk and mission impact.

Implementation Notes (Optional)

Short guidance on sequencing, rollout, and how to reduce user friction while improving control.

This is not a full compliance program. It is a practical starting point that helps teams move from requirements to enforceable policy decisions.

In practice, it helps teams establish a defensible baseline, reduce workarounds that weaken security, and make policy decisions easier to explain internally.

How To Use This In 15 Minutes Or Less

Step 1	**Choose one workflow to secure first** Examples include contractor access, a sensitive SaaS application, or a privileged admin session.
Step 2	**Select the minimum set of controls that make that workflow defensible.** Start small and intentional. Avoid turning every policy into a blanket restriction.
Step 3	**Adopt a starter set as the baseline.** Use it as a default stance, then adjust only where risk or mission sensitivity warrants it.
Step 4	**Tighten or loosen based on risk and friction.** If controls create workarounds, you often end up with less security and worse visibility. Optimize for safe adoption.

The Mapping Model

This pack uses one practical model:

What you are protecting

The data and workflow that matter most.

From what risk

The common ways that workflow fails, leaks, or is abused.

With what "last-mile" controls

The controls enforced at the point of work in the browser, including what users can and cannot do.

What evidence you can produce

The proof points you can show for audit readiness and incident response.

Control Categories

Each category includes three things: the goal, the default stance, and when to tighten.

Data movement controls	Controls that reduce accidental or intentional data exfiltration. • Copy and paste boundaries • Downloads • Printing
Access assurance controls	Controls that strengthen confidence that the right person is accessing the right resource under the right conditions. • Step-up authentication for sensitive applications (when needed) • Session handling, including timeouts and re-authentication patterns
Visibility and investigation	Controls that improve what you can reconstruct during reviews, investigations, and response. • Activity logging expectations (high-level) • What to capture for incident review (simple and actionable)

Starter Sets

These starter sets are designed to feel safe, not extreme. They are meant to establish a baseline and then evolve as you learn.

Starter Set 1: Contractor or third-party access	A baseline for higher-risk users and mixed device environments. • Conservative download defaults • Clear copy and paste boundaries • Strong session rules
Starter Set 2: Sensitive SaaS workflows (PII, PHI-like, or regulated data)	A baseline for high-impact data in common web applications. • Restrict downloads to approved destinations • Tighten print controls • Apply a basic step-up authentication pattern if required
Starter Set 3: Privileged admin browser sessions	A baseline for high-trust users performing high-risk actions. • Tightest copy, paste, and download stance • Strong re-authentication patterns • Increased logging expectations

Evidence Checklist

Use this as a lightweight set of artifacts to support approvals, audits, and investigations.

Audit Readiness

- [ ] Written policy intent for each control category (data movement, access assurance, visibility)
- [ ] A documented baseline (which starter set you used, and why)
- [ ] Proof that controls are enforced (screenshots or exports of key policy settings)
- [ ] A short record of exceptions (what was allowed, for whom, for how long, and who approved it)
- [ ] A change log for policy updates (what changed, when, and the rationale)

Incident Review

- [ ] Timeline of relevant user activity (who, what, when)
- [ ] The affected workflow and application context (which app, which data path, which session type)
- [ ] The policy state at the time of the incident (what controls were in effect)
- [ ] A record of escalations and decisions (who approved next steps, and when)
- [ ] Evidence package you can hand to stakeholders (export or report format that can be shared with Security and Legal)

Want to see what this looks like for your environment?

Visit Island on The Trading Post and click Connect with Island.

REDLEIF Island

2026