**CERT-01 — Independent Certifications Pack (ISO 27001 / SOC 2 Binder)**

**Intent**  
Package all compliance evidence (security, privacy, continuity) into an auditor-ready binder your customers can accept during procurement.

**Actors**  
Compliance Lead • Security Architect • DPO/Legal • Audit Coordinator • Audit Vault

**Preconditions**

* Security controls implemented (RBAC/SoD, logging, encryption, backups, DR drills).
* Policies approved (Access, Change Mgmt, Incident Response, Vendor Mgmt, Data Retention/Residency).
* Reports available: BCP drill, pen-test, access reviews, SoD attestations.

**Flow (happy path)**

1. **Control Map**
   * Map ISO 27001 Annex A & SOC 2 (Security/Availability/Confidentiality) controls → your proofs (from OPS & ADD stories).
   * Assign **control owners** and review cadence.
2. **Evidence Collection**
   * Pull signed artifacts: BCP Proof Bundle, Override Notarizations, Access Review results, DR drill outputs, Retention/Residency reports, Pen-test & remediation log, Secrets rotation report.
   * Freeze each with a **Binder Receipt** (hash + time + owner).
3. **Document Set**
   * Policies (approved & versioned), Procedures (runbooks), Architectures (diagrams), Data Inventory, DPIA/ROPA, Vendor/Subprocessor list, Change logs, Release notes.
4. **Redaction & Sharing**
   * Produce **Customer Redacted** pack (no sensitive IP/keys).
   * Host in read-only portal; watermark; expiry links; access logging.
5. **Mock Audit**
   * Internal auditor walks a mini-audit; gaps → action items with owners/dates.

**Edge cases**

* Missing evidence/time-boxed controls → document compensating controls + improvement plan.
* Region-specific requirements → add Residency Addendum per region (EU/IN/US).

**Done when**

* Binder index complete; 100% controls have a mapped proof; mock audit passes; redacted pack accessible with audit logging.

**Deliverables**  
Control-to-Evidence Matrix, Evidence Binder (internal), Redacted Customer Pack (PDF/portal), Binder Receipt.

s