

Supplement S1 — Auditor Playbook

Aggressive Audit Gauntlet (public-safe) — Mirrors Appendix B8 of Kingdom Conformance RFC v1.3.6

Purpose: a high-stringency buyer/auditor checklist intended to *falsify* (not merely confirm) L1+ replay claims and L2+ enforcement claims within a declared audit window.

Inputs (minimum): Conformance Statement(s); sampled Conformance Pack(s) + authorized evidence-handle access; validator test vectors (incl. negative and freshness-boundary); and (for L2+) side-effect inventory to reconcile permits/receipts to observed actions.

Check	What to attempt	Fail signals	Finding map
G0	Conformance Statement completeness and scope boundaries are unambiguous.	Missing required fields; scope/control points/receipt types unclear or internally inconsistent.	F1 Structural
G1	Coverage reconciliation: every claimed coverage unit (receipt type × control point × scope) has replay-verifiable evidence in the audit window.	Coverage claimed but no corresponding receipts/gate evidence for the audit window.	F3 Coverage gap
G2	Offline replay: independent verifier reproduces recorded PASS/FAIL/HOLD and reason codes under the pinned policy/validator versions.	Replay decision differs; reasons differ; required evidence handles cannot be resolved under declared bindings.	F2 Replay mismatch
G3	Freshness boundary: stale/expired prerequisites deterministically yield HOLD (or FAIL if policy requires) and do not allow sensitive side effects.	Stale evidence still yields PASS; or HOLD/FAIL does not block sensitive side effects.	F4 Freshness breach (and F5 if enforcement fails)
G4	Side-effect reconciliation (L2+): no side effect in scope occurs without a valid, in-scope Permit minted after PASS and validated at the relevant control point.	Observed side effect with missing/invalid/out-of-scope permit; permit minted before PASS.	F5 Enforcement failure
G5	Fail-closed drills (L2+): at each covered control point, missing/unknown/unverifiable prerequisites block the action (no fail-open on errors or degraded conditions).	Control point allows action on error/degraded mode; missing prerequisites do not block.	F5 Enforcement failure
G6	Change-control integrity: policy/validator/CanonicalFormID version resolution and signed change history are replay-stable; required registry snapshot references are present and verifiable; ambiguous identifiers yield HOLD, not PASS.	Ambiguous/unstable version resolution; missing registry snapshot refs; unknown IDs still PASS.	F2 Replay mismatch / F6 Reason-code instability
G7	Reason-code stability: reason-code meanings do not change without a policy/validator version bump, and the applicable Reason Code Registry snapshot reference (or equivalent) is available for audit.	Reason code meaning changes without version bump; or no resolvable reason-code registry snapshot for the audit window.	F6 Reason-code instability
G8	Revocation propagation (L3 or if claimed): revoked approvals become operationally effective at gates within the buyer-selected revocation latency objective.	Revoked approvals still usable at gates beyond stated objective.	F5 Enforcement failure

Notes: (1) Informative and implementation-agnostic; does not prescribe cryptography or internal controls. (2) Treat unverifiable artifacts as HOLD/FAIL per policy; do not "paper over" missing evidence. (3) Map findings to F1–F6 for comparability across suppliers.