Controls Mapping Pack

SOC 2 / ISO 27001 / NIST CSF — Evidence Pointer Crosswalk

Procurement-friendly crosswalk: common control language mapped to MVG mechanisms (Verify -> Permit -> Gate; fail-closed), with evidence pointers and offline verification hints. Informational only; auditors remain authoritative for control conclusions.

Disposition glossary

PASS — signatures verify; execution permitted only within declared scope/lease.	HOLD — evidence missing/ambiguous or human approval required; execution MUST NOT proceed.	FAIL — integrity mismatch or policy violation; execution blocked; incident MUST be logged.

Generated: 2026-02-27 | Scope: Public • procurement-safe • Informational only; not a certification or audit opinion.

Canonical evidence entry points

Start here	/trust-center/ | /.well-known/mvg-procurement-ticket-pack.dsse.json | /verify/ | /trust/transparency/

Full table (CSV): /downloads/controls-mapping/controls_mapping_v1.csv • Current PDF: /downloads/controls-mapping/controls_mapping_v1.pdf

Receipt scaffold (optional): /downloads/controls-mapping/SHA256SUMS.controls_mapping (+ .asc)

Legend
• Evidence pointers are designed to be replayable offline (DSSE, proofs, receipts).
• Recommended workflow: Trust Center → DSSE viewer → Verify offline → record PASS / HOLD / FAIL in the ticket (fail-closed).
• Design upgrade: this v2 layout includes a per-row “Anchor ID” so tickets and reviews can reference rows unambiguously.
• To verify this mapping pack itself, validate the published checksums file and its detached signature (once signed).

Controls crosswalk (full table)

SOC 2 / ISO 27001 / NIST CSF controls mapped to MVG mechanisms, evidence pointers, and offline verification hints.

Control	Control intent	MVG mechanism	Evidence & offline verify (hint)	Expected outputs
SOC 2 CC8.1 / ISO 27001:2022 A.8.32 / NIST CSF PR.IP-3	Change management is authorized, tested, and traceable.	Site Release receipts + append-only transparency; FAIL-closed (uncertainty ⇒ HOLD).	Evidence: /trust/site-release/ /trust/transparency/ /.well-known/mvg-procurement-ticket-pack.dsse.json Verify: Open DSSE viewer -> verify pointers; run /verify/ offline; expect PASS only if signatures + hashes match. Anchor ID: CMAP-0001	PASS: signatures verify + hashes match · HOLD: missing/unverifiable · FAIL: mismatch/tamper

Control	Control intent	MVG mechanism	Evidence & offline verify (hint)	Expected outputs
SOC 2 CC6.1 / ISO 27001:2022 A.5.15 / NIST CSF PR.AC-1	Logical access is restricted to authorized identities.	Permit-to-act gate + reason codes; no silent execution without receipts.	Evidence: /solutions/agentic/ /verify/ /trust/reason-codes/ Verify: Verify Conformance Pack outputs (PASS/FAIL/HOLD) in offline verifier. Anchor ID: CMAP-0002	PASS: permitted actions only · HOLD: missing evidence · FAIL: unauthorized action evidence
SOC 2 CC6.3 / ISO 27001:2022 A.5.18 / NIST CSF PR.AC-4	Least privilege and segregation of duties.	Offline production keys + governance stop authority; release ceremony enforces separation.	Evidence: /governance/ /.well-known/mvg-governance.json /trust/site-release/ Verify: Review governance receipt; verify detached signature when GO-LIVE; confirm HOLD behavior until signed. Anchor ID: CMAP-0003	PASS: receipt verifies · HOLD: unsigned/unverifiable by design · FAIL: signature mismatch
SOC 2 CC7.1 / ISO 27001:2022 A.8.16 / NIST CSF DE.CM-1	Monitoring detects anomalies and integrity issues.	Deterministic verification outputs (PASS/FAIL/HOLD) surface anomalies as reason codes.	Evidence: /verify/ /trust/site-release/ /trust/reason-codes/ Verify: Run verifier; confirm mismatches produce FAIL and missing proofs produce HOLD. Anchor ID: CMAP-0004	PASS/HOLD/FAIL are deterministic and replayable

Control	Control intent	MVG mechanism	Evidence & offline verify (hint)	Expected outputs
SOC 2 CC7.2 / ISO 27001:2022 A.8.8 / NIST CSF ID.RA-1	Vulnerabilities are identified and managed.	Public disclosure surface + escalation channels; signed identity receipts reduce phishing risk.	Evidence: /.well-known/security.txt /legal/security-disclosure/ /company/ Verify: Check security.txt + disclosure policy; verify official channels match @meridianverity.com. Anchor ID: CMAP-0005	PASS: channels consistent · HOLD: ambiguity in channels · FAIL: conflicting official channels
SOC 2 CC7.3 / ISO 27001:2022 A.5.24 / NIST CSF RS.RP-1	Incident response plan exists with escalation path.	Governance descriptor defines who can stop a release and escalation path; fail-closed posture.	Evidence: /governance/ /.well-known/mvg-governance.json /trust/security-review/ Verify: Open governance receipt + Security Review Packet (public); confirm escalation contacts. Anchor ID: CMAP-0006	PASS: defined escalation + contacts · HOLD: missing receipt · FAIL: contradictory contacts
SOC 2 CC2.1 / ISO 27001:2022 A.5.1 / NIST CSF GV.PO-1	Policies are communicated and maintained.	Policy surfaces are public + canonical; signed receipts are authoritative.	Evidence: /trust-center/ /legal/ /.well-known/mvg-company.json Verify: Use Trust Center canonical links; verify receipts when signatures are published. Anchor ID: CMAP-0007	PASS: canonical links resolve · HOLD: missing signature · FAIL: mismatch

Control	Control intent	MVG mechanism	Evidence & offline verify (hint)	Expected outputs
SOC 2 CC1.2 / ISO 27001:2022 A.5.2 / NIST CSF GV.RR-1	Governance oversight and assignment of responsibilities.	Governance receipt + stop authority; audit-ready responsibility chain.	Evidence: /governance/ /.well-known/mvg-governance.json /trust/identity-receipts/ Verify: Verify governance descriptor; follow runbook for signature verification. Anchor ID: CMAP-0008	PASS when signed; otherwise HOLD by design
SOC 2 CC5.2 / ISO 27001:2022 A.5.33 / NIST CSF PR.IP-7	Risk assessment and continuous improvement.	Transparency log + annual Safety & Impact reporting methodology (public).	Evidence: /impact/ /trust/transparency/ Verify: Review published metric definitions; confirm they are tied to receipts and verifier outputs. Anchor ID: CMAP-0009	PASS: methods reproducible · HOLD: missing definitions · FAIL: unverifiable claims
SOC 2 CC6.6 / ISO 27001:2022 A.8.9 / NIST CSF PR.IP-1	Configuration management is controlled and auditable.	Pinned artifacts + deterministic bundles; integrity mismatch escalates to FAIL.	Evidence: /trust/site-release/ /transparency/procurement-ticket-pack/prod/proofs/LATEST.json Verify: Verify SRI/pinned hashes; confirm verifier outputs FAIL on mismatch. Anchor ID: CMAP-0010	PASS: matches · FAIL: mismatch · HOLD: missing pointer

Control	Control intent	MVG mechanism	Evidence & offline verify (hint)	Expected outputs
SOC 2 CC8.1 / ISO 27001:2022 A.5.19 / NIST CSF ID.SC-4	Supplier relationships and external dependencies are managed.	No third-party scripts; pinned build inputs; verifiable supply-chain posture.	Evidence: /trust/site-release/ /trust/security-review/ Verify: Confirm CSP/no 3rd-party; verify release receipts. Anchor ID: CMAP-0011	PASS: posture matches docs · FAIL: unexpected external deps
SOC 2 P4 / ISO 27001:2022 A.5.34 / NIST CSF PR.DS-1	Privacy and data protection are documented and enforced.	Controlling privacy policy is published and hash-pinnable; receipts are authoritative.	Evidence: /legal/privacy/ /transparency/procurement-ticket-pack/prod/proofs/LATEST.json Verify: Compare sha256 of controlling privacy PDF to transparency entry artifacts. Anchor ID: CMAP-0012	PASS: hash matches · FAIL: mismatch · HOLD: missing proof
SOC 2 CC4.2 / ISO 27001:2022 A.8.15 / NIST CSF GV.IM-1	Evidence and audit trails support oversight.	DSSE pointers + evidence packs + inclusion proofs (replayable, offline).	Evidence: /trust/dsse-viewer/ /.well-known/mvg-procurement-ticket-pack.dsse.json /trust/transparency/ Verify: Use DSSE viewer; validate pointers; verify inclusion proof and expected outputs. Anchor ID: CMAP-0013	PASS if artifacts + proofs verify; else HOLD/FAIL

Control	Control intent	MVG mechanism	Evidence & offline verify (hint)	Expected outputs
SOC 2 CC9.2 / ISO 27001:2022 A.5.29 / NIST CSF ID.IM-1	Vendor diligence and authenticity are established.	Signed identity receipts (Company + Governance) + anti-phishing channel policy.	Evidence: /company/ /governance/ /trust/identity-receipts/ Verify: Verify detached signatures (gpg --verify) and confirm domains/channels. Anchor ID: CMAP-0014	PASS: signatures verify · HOLD: unsigned by design · FAIL: signature mismatch
ISO 27001:2022 A.5.30 / NIST CSF PR.IP-2	Business continuity posture avoids silent failure.	Fail-closed: uncertainty never yields silent PASS; HOLD forces review.	Evidence: /trust/site-release/ /trust/reason-codes/ Verify: Confirm HOLD conditions are explicit in docs and enforced by verifiers. Anchor ID: CMAP-0015	HOLD on uncertainty; PASS only with complete, verifiable evidence