

# Control Mapping Appendix (Public)

How the Defensible Execution Evidence Pack can support audit evidence collection. This mapping is illustrative and does not certify compliance.

Evidence pack construct	SOC 2 (TSC)	ISO/IEC 27001:2022 (Annex A)	NIST 800-53	What it demonstrates
Moment That Matters resolution (mtm_snapshot.json)	CC7.2, CC7.3	5.7 Threat intelligence; 5.30 ICT readiness for business continuity	IR-4, RA-3	The system detects and classifies high-consequence decision points before action.
Named authority chain (authority_contract.json)	CC6.1, CC6.2	5.15 Access control; 5.16 Identity management; 5.17 Authentication information	AC-2, AC-3, AC-6	Who held jurisdiction at the moment of action; authority is explicit and reviewable.
Delegation bounds (scope, TTL, caps)	CC6.2, CC7.2	5.18 Access rights; 8.9 Configuration management	AC-6, CM-3	Automation acts only within defined limits; no silent privilege expansion.
Execution-time enforcement record (enforcement_record.json)	CC7.2, CC7.3	8.9 Configuration management; 8.15 Logging	CM-3, AU-12	Controls are applied in the execution path, not just documented.
Escalation path + time-boxes	CC7.3, CC7.4	5.24 Incident management planning and preparation; 5.28 Collection of evidence	IR-4, IR-5	Uncertainty triggers defined escalation; response is engineered, not discretionary.
Audit export (audit_export.ndjson)	CC7.2, CC7.3	8.15 Logging; 8.16 Monitoring activities	AU-2, AU-3, AU-12	A structured, ingestible record of what was proposed vs executed and why.
Policy trace with doctrine versioning (policy_trace.ndjson)	CC7.2	5.1 Policies; 8.9 Configuration management	CM-3, AU-3	Which checks fired, under what versioned doctrine; supports change review and auditability.
Provenance chain (provenance_chain.json)	CC7.2, CC7.3	8.12 Data leakage prevention; 8.23 Web filtering (as relevant)	AU-3, SI-4	What the system relied on (model output, tool calls) and integrity of the chain.
Integrity (manifest.json + signature)	CC7.2	5.28 Collection of evidence; 8.15 Logging	AU-9, AU-12	Pack is tamper-evident; evidence object can be trusted without access to source systems.
Board View / Regulator View PDFs	CC1.2, CC7.2	5.1 Policies; 5.24 Incident mgmt; 5.28 Evidence collection	PM-6, IR-4	Human-readable proof for executives and regulators: action, authority, bounds, escalation.

Disclaimer: This document describes how the evidence pack may support your control evidence. It does not constitute legal advice and does not certify compliance.

Contact: [founder@judgementspine.com](mailto:founder@judgementspine.com)

