VERITY SYSTEMS

DMS Module — SOC 2 Control Mapping

- This document maps the VERITY DMS (V1 + V2) architecture against SOC 2 Trust Services Criteria.
- Coverage includes Security, Availability, Processing Integrity, and Confidentiality domains.
- Threat references align with the internal DMS Threat Matrix (T01–T30).

SOC2 Control	Domain	DMS Implementation Summary	Threat Coverage
CC6.1	Logical Access	Tenant isolation + RBAC + Folder ACL enforcement	T01, T09, T28
CC6.2	Authorization	workflowEngine-only status transitions, review validation	T03, T11, T12
CC6.3	Privileged Access	Admin-only ACL updates + guarded audit export	T10, T22
CC7.1	Monitoring	Global AuditLog + canonical action events	T21, T23
CC7.2	Change Management	Additive migrations + audited permission changes	Workflow & ACL changes
CC9.1	Risk Mitigation	Transactional updates + concurrency-safe logic	T04, T30
PI1.1	Processing Integrity	Multi-stage approval validation inside transaction	T04, T12
PI1.2	Data Integrity	Unique constraints + no direct status mutation	T03, T06
C1.1	Confidentiality	Signed URLs + private storage + tenant-prefixed keys	T01, T19
A1.2	Availability	Streaming audit export + idempotent scheduler	T18, T29

Conclusion

- Current architectural readiness: Strong for Security, Logical Access, Processing Integrity, and Confidentiality.
- Operational enhancements required for full SOC 2 Type II maturity: Legal Hold, Retention enforcement, Audit hash-chaining, centralized monitoring.
- DMS V2 architecture supports expansion to full compliance without structural refactor.