SOC 2 Control Matrix – Portfolio Artifact

This sample control matrix demonstrates ability to align organizational controls with SOC 2 Trust Services Criteria (TSC), identify evidence, assign owners, and set review frequencies. It shows readiness for compliance and audit-focused GRC roles.

TSC	Control	Evidence Example	Owner	Frequency
CC6.1 – Logical Access	MFA enforced for all remote logins	IdP MFA config screenshot; Access Policy	IT Security	Continuous
CC6.6 – User Access Reviews	Quarterly access reviews for critical systems	Review notes; closure tickets	IT Manager	Quarterly
CC7.2 – Logging & Monitoring	Centralized logging + alerting via SIEM	SIEM dashboard; incident tickets	Security Ops	Continuous
CC9.2 – Data Retention	Retention policy; secure disposal of logs	Policy doc; storage lifecycle settings	Compliance Lead	Annual
A1.2 – Availability	Daily DB backups with tested recovery	Backup logs; restore test results	IT Infrastructure	Daily

Note: SOC 2 criteria are organized under Security (common) and optional categories such as Availability, Confidentiality, Processing Integrity, and Privacy. This matrix provides a sample subset for demonstration.