Posture Scorecard

Document: SS-SOC2-001C **Version:** 1.0 **Date:** 2026-02-28

Owner: Skyes Over London LC - Security & Trust Office

Applies to: All systems handling client/customer data under SKYE governance

Purpose

A fast, evidence-backed snapshot of SOC 2 posture under SKYE. Use this scorecard to assign a posture tier, surface gaps, and enforce production gates.

System identification

System	_____
Owner	_____
Date	_____
Assessor	_____
Target Tier (Level 1/2/3)	_____
Current Tier (assessed) (Level 0/1/2/3)	_____

Scoring rules

Each domain is scored 0-5. 0 = Unknown/no owner/no evidence. 1 = Defined only (docs exist; not operating). 2 = Partial operating (inconsistent evidence). 3 = Operating (consistent evidence for 30-90 days). 4 = Strong operating (evidence for full period; minimal exceptions). 5 = Audit-grade sustained (review cadence met; exceptions rare and closed fast).

Domain scores

Domain	Score (0-5)	Notes / Evidence link
SS-IAM (Identity & Access)	____	_____
SS-CHG (Change Management)	____	_____
SS-OBS (Logging/Monitoring/Alerting)	____	_____
SS-VULN (Vulnerability & Patch)	____	_____
SS-IR (Incident Response)	____	_____
SS-DATA (Data Protection & Secrets)	____	_____
SS-VEND (Vendor Risk)	____	_____
SS-AVL (Availability/DR) (if applicable)	____	_____
SS-CONF (Confidentiality) (if applicable)	____	_____
SS-PI (Processing Integrity) (if applicable)	____	_____
SS-PRIV (Privacy) (if applicable)	____	_____
SS-AI (AI Add-On Controls) (if applicable)	____	_____

Tier mapping (SKYE)

Level 0: Any mandatory domain scored 0-1. Level 1: Mandatory domains average at least 2, but evidence is incomplete or inconsistent. Level 2: Mandatory domains average at least 3 AND no mandatory domain is below 3. Level 3: Mandatory domains average at least 4 AND no mandatory domain is below 4 AND review cadences are current.

Risk flags (auto-fail gates)

If any of the following are true, the system cannot be Level 2+ until resolved or an SS-SOC2-001D exception is approved:

- No MFA on privileged access.
- No centralized audit logs for admin actions.
- No incident response process.
- No vulnerability scanning or remediation tracking.
- Secrets committed to repo or unmanaged secrets sprawl.
- No access review within required cadence.

Top 10 gaps

Gap	Owner	Due
1) _____	_____	_____
2) _____	_____	_____
3) _____	_____	_____
4) _____	_____	_____
5) _____	_____	_____
6) _____	_____	_____
7) _____	_____	_____

Gap	Owner	Due
8) _____	_____	_____
9) _____	_____	_____
10) _____	_____	_____

Decision

Production Status (Approved / Approved with Conditions / Not Approved)	_____
Conditions (if any)	_____
Next Review Date	_____