SOC 2 Posture Checklist

Document: SS-SOC2-001A **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 structured, evidence-focused checklist used to measure and enforce SOC 2 posture under the SKYE Standard. This checklist is designed for fast assessments, consistent control coverage, and audit-ready documentation.

How to use: For each requirement, mark one status box (Done, Partial, Not, or N/A). Any Not item requires either remediation with a due date or an approved SS-SOC2-001D exception.

Completion gate (SKYE enforcement)

To reach Level 2: All Mandatory sections 1-7 must be Done or Partial with remediation due dates. No open Not items without an approved exception. To reach Level 3: Mandatory sections are Done, required modules applicable are Done, and evidence is complete for the audit period with current review cadences.

Section 0 - System Identification (Required)

Done	Partial	Not	N/A	Requirement
				System name: _____
				System owner (name + role): _____
				Business purpose: _____
				Data classification: Public / Internal / Confidential / Restricted
				Contains personal data? Yes / No (If yes, Privacy module applies)
				Environments (Dev / Staging / Prod): _____

Done	Partial	Not	N/A	Requirement
				Hosting/providers (critical): _____
				Production go-live date (or planned): _____
				Posture tier target: Level 1 / Level 2 / Level 3
				Last posture review date: _____

1 - Identity & Access Control (SS-IAM) (Mandatory)

Done	Partial	Not	N/A	Requirement
				MFA enforced for all privileged accounts (admin, cloud consoles, DB, CI/CD).
				No shared privileged accounts; named accounts only.
				Role-based access control (RBAC) defined for app and infrastructure.
				Least privilege implemented (no broad owner roles unless justified).
				Joiner/Mover/Leaver process documented and used.
				Offboarding SLA defined and met (target: same-day for privileged access).
				Quarterly access reviews completed (monthly for high-risk systems).
				Break-glass access exists, logged, and reviewed.
				API keys/tokens are scoped and rotated; no long-lived secrets without justification.
				Service accounts are limited, monitored, and reviewed.

2 - Change Management (SS-CHG) (Mandatory)

Done	Partial	Not	N/A	Requirement
				All production changes tracked (PR/ticket required).
				Approvals required for production changes (defined approver role).
				Separation of duties for sensitive changes (when feasible).
				CI checks enforced (lint/test/build; dependency scan where applicable).
				Deployment logs retained and searchable.
				Rollback plan exists for production releases.
				Emergency changes process exists and is audited.
				Infrastructure changes are version-controlled (IaC or equivalent traceability).

3 - Logging, Monitoring, Alerting (SS-OBS) (Mandatory)

Done	Partial	Not	N/A	Requirement
				Centralized logging enabled for auth, admin actions, and application events.
				Audit logs enabled for cloud provider / identity provider / database.
				Alerts configured for auth anomalies (MFA bypass, impossible travel, brute force).
				Alerts configured for availability and error rate thresholds.
				Log retention configured per risk (minimum policy specified).
				Time synchronization enabled (NTP) for accurate timestamps.
				Access to logs restricted and reviewed.
				Evidence of alert testing exists (at least quarterly).

4 - Vulnerability & Patch Management (SS-VULN) (Mandatory)

Done	Partial	Not	N/A	Requirement
				Dependency scanning enabled (SCA).
				Vulnerability triage process defined (severity + owner + SLA).
				Patch SLAs defined (example: Critical 7d, High 14d, Medium 30d, Low 90d).
				OS/container/base image patching documented.
				Periodic vulnerability scans performed (cadence defined).
				Remediation tickets tracked to closure.
				Secrets scanning enabled for repos and build pipelines.

5 - Incident Response (SS-IR) (Mandatory)

Done	Partial	Not	N/A	Requirement
				Incident severity levels defined (SEV scale).
				On-call/escalation path defined and current.
				Incident response runbook exists and accessible.
				Evidence of at least one tabletop exercise annually (quarterly high-risk).
				Post-incident review process exists (root cause + corrective actions).
				Incident logs/tickets retained.
				Client notification criteria documented (if applicable).

6 - Data Protection & Secrets (SS-DATA) (Mandatory)

Done	Partial	Not	N/A	Requirement
				TLS enforced for all network traffic (external and internal where feasible).
				Data-at-rest encryption enabled for databases and object storage (where supported).
				Secrets stored in approved secret manager / environment vars; never committed to code.
				Secret rotation policy defined and followed.
				Data classification policy applied to system data types.
				Data retention and deletion policy implemented.
				Backups encrypted and access-controlled.
				Data access is logged for sensitive datasets.

7 - Vendor & Third-Party Risk (SS-VEND) (Mandatory)

Done	Partial	Not	N/A	Requirement
				Vendor inventory maintained for critical vendors (cloud, auth, DB, payments, email).
				Vendor access is least-privilege and reviewed.
				SOC reports or security attestations collected when available (critical vendors).
				Subprocessor list maintained (if handling customer data).
				Contractual security requirements tracked (SLAs, breach notice terms).

8 - Availability & Disaster Recovery (SS-AVL) (Required if uptime promised / critical)

Done	Partial	Not	N/A	Requirement
				Uptime objective defined (SLO/SLA).
				Backups scheduled and monitored.
				Restore test performed at least annually (quarterly for critical).
				DR plan documented (RTO/RPO targets).
				Redundancy implemented where required.
				Capacity monitoring in place.

9 - Confidentiality (SS-CONF) (Required if sensitive business data)

Done	Partial	Not	N/A	Requirement
				Data classification applied and enforced.
				Sensitive data access restricted and reviewed more frequently.
				DLP controls applied where appropriate (email/storage).
				Field-level protections used where needed (masking/tokenization).

10 - Processing Integrity (SS-PI) (Required if correctness is contractually important)

Done	Partial	Not	N/A	Requirement
				Input validation and error handling standards defined.
				Reconciliation or audit trails for critical transactions.
				Job/queue retries are safe and monitored.
				Data integrity checks exist for critical flows.

11 - Privacy (SS-PRIV) (Required if personal data)

Done	Partial	Not	N/A	Requirement
				Privacy notice and data use purpose defined.
				Data subject request (DSR) process defined (access/delete/export).
				Data minimization enforced (collect only necessary data).
				Consent handling documented where required.
				Retention policy aligns with privacy requirements.

12 - AI Add-On Controls (SS-AI) (Required if AI/LLM is used)

Done	Partial	Not	N/A	Requirement
				Model access governed (scoped keys, caps, audit logs).
				Sensitive data handling rules defined (no secrets in prompts).
				Output logging for high-impact workflows (with redaction where required).
				Human review for high-risk decisions (when applicable).
				Prompt/version changes follow change control.
				Abuse monitoring and rate limiting enabled.