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.

Evidence Index Template

Document: SS-SOC2-001B **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 single index that maps each control to proof artifacts. This is the SKYE receipts binder: every control must have evidence that is time-stamped, attributable, and retrievable on demand.

System header (complete before use)

System Name	_____
System Owner	_____
Review Period (From - To)	_____
Posture Tier (Level 1/2/3)	_____
Evidence Repository Location (link/path)	_____

Evidence record template (repeat per control)

Create one evidence record per control. Store each artifact in a stable location and link it here.

Evidence ID (SKYE-[System]-[Domain]-[Number])	_____
Control Domain (SS-IAM / SS-CHG / ...)	_____
Control Name	_____
Control Description (1-3 sentences)	_____

Evidence Type (Screenshot/Export/Log/Ticket/Report/Config/Policy/Runbook/Training/Test)	_____
Evidence Source (tool/system)	_____
Collection Method (Manual/Automated/Scheduled/API)	_____
Collection Cadence (Continuous/Daily/Weekly/Monthly/Quarterly/Annually)	_____
Time Range Covered	_____
Storage Location (exact link/path)	_____
Owner (responsible)	_____
Verifier (checks)	_____
Last Verified Date	_____
Result (Pass/Fail/Needs Follow-up)	_____
Notes (exceptions, anomalies, follow-ups)	_____

Minimum evidence set (by domain)

These are the minimum receipts expected when the domain applies. Add system-specific evidence as needed.

SS-IAM

- MFA enforcement proof
- Access review export
- Offboarding tickets (sample)
- Privileged role list

SS-CHG

- PR approval logs
- Deployment logs
- Emergency change record
- Rollback evidence (example)

SS-OBS

- Audit log enabled proof
- Alert rules export/screenshot
- Incident alert example
- Retention settings proof

SS-VULN

- Scan reports
- Remediation tickets
- Patch cadence evidence
- Secrets scan status

SS-IR

- Incident response plan
- On-call roster
- Tabletop notes
- Post-incident review example

SS-DATA

- TLS configuration proof
- Encryption-at-rest proof
- Secret storage proof
- Retention and deletion settings

SS-VEND

- Vendor inventory
- Vendor access review
- Security attestations (when available)

SS-AVL

- Backup schedule proof
- Restore test result
- DR plan (RTO/RPO)

SS-PRIV

- Privacy process docs
- DSR log
- Retention mapping to requirements

SS-AI

- Key governance and caps
- Prompt change history
- Output logging/redaction evidence

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	_____

Exception Form

Document: SS-SOC2-001D **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 controlled method to allow temporary non-compliance without hiding risk. Every exception must be time-bound, compensated, owned, and tracked to closure with evidence.

Exception identification

Exception ID (SS-SOC2-EX-YYYY-###)	_____
Date Submitted	_____
Submitted By	_____
System Name	_____
System Owner	_____
Control Domain (SS-IAM / SS-CHG / ...)	_____
Control Reference (e.g., SS-SOC2-001A 1.7 Access Review Cadence)	_____

Exception type (select one)

☐	Temporary gap	☐	Legacy constraint	☐	Vendor limitation
☐	Emergency change	☐	Other	☐	

What is being excepted (clear description)

_____

_____

_____

Why the exception is needed (business/technical justification)

_____

_____

_____

Risk statement

Likelihood: Low / Medium / High Impact: Low / Medium / High

Risk summary (2-5 sentences):
_____
_____

Compensating controls (what we do instead, right now)

1) _____
2) _____
3) _____

Scope of impact

Environments affected (Dev/Staging/Prod)	_____
Users affected (Internal only / Customers / Partners)	_____
Data affected (Public/Internal/Confidential/Restricted)	_____
Geography/regulatory impact (if any)	_____

Remediation plan (mandatory)

Fix owner	_____
Target completion date	_____
Validation method (how we prove it is fixed)	_____

Action steps:
- Step 1: _____
- Step 2: _____
- Step 3: _____

Exception duration

Start date	_____

End date (must be time-bound)	_____
Review cadence during exception (Weekly / Monthly)	_____

Approvals

System Owner (name + date)	_____
Security & Trust Office Approver (name + date)	_____
Executive Approver (required for High risk) (name + date)	_____

Closure

Date closed	_____
Closure evidence link/path	_____
Notes	_____