

SOC 2 controls list

82 example controls across 5 Trust Services Criteria families, each tied to criterion IDs, the evidence an auditor may request, and the gap auditors flag most.
Library updated 2026-10-08.

These are example controls written by SOC2Auditors.org. They name criterion IDs only and do not prove coverage of any criterion. Confirm applicability, evidence and testing with your CPA firm.

Security controls (CC1–CC9)

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC1.1 Integrity and ethical values C1.1 Identifying and protecting confidential information	GV-01 Publish a code of conduct and a confidentiality agreement. Every employee and contractor signs both before receiving system access and re-acknowledges the code of conduct each year.	- Signed code of conduct and confidentiality agreement for each hire, dated on or before the day access was granted (HR system) - Annual acknowledgment report listing every active employee and contractor with the date each signed (HR system) - Current code of conduct with its approval date and the consequences for violations (Policy repository)	A signed agreement for every person hired during the period and a completed annual acknowledgment cycle, so the auditor can sample both new hires and existing staff.	Annual	New hires sign days or weeks after they were given system access, or contractors are left out of the acknowledgment.
CC1.2 Board oversight	GV-02 Brief your board on security risks, incidents and control status at least annually, and record questions and agreed actions in minutes. With no board, name an outside advisor or investor to do this; founders reviewing their own work are not independent.	- Board or advisory charter, or a written note of who provides oversight and how independent they are from management (Board and management records) - Dated minutes or briefing deck showing security and risk discussed, with the questions raised and follow-up actions (Board and management records)	Minutes for each oversight meeting due in the period, showing security on the agenda as often as the charter or policy says.	Annual	Security never reaches the board agenda, or the minutes record a presentation with no questions, decisions or follow-up.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC1.3 Structure, reporting lines and authority	GV-03 Maintain an org chart and written role descriptions that name who owns security, who they report to, and who may approve access, changes and risk exceptions.	- Current org chart with reporting lines, dated or under version control (HR system) - Responsibility matrix naming the security owner and the approvers for access, changes and risk acceptance (Policy repository)	Org chart versions or HR records showing reporting lines kept current as people joined, left or changed roles during the period.	Annual	Nobody is formally named as security owner, so approvals in tickets come from people with no assigned authority to give them.
CC5.3 Policies and procedures	PL-01 Keep written security policies covering topics such as access, change, incident response, vendors, data handling and acceptable use, with procedures that put each into practice. Management approves them and reviews them at least annually.	- Policy set with version history, owner, approval date and next review date for each policy (Policy repository) - Record of management approval for the latest review, such as a signed approval page or approval ticket (Board and management records) - Procedures and runbooks that carry out each policy, such as the offboarding checklist and incident runbook (Policy repository)	Each policy reviewed and approved on its stated cadence during the period, and procedures in use that match the approved versions.	Annual	Policies are templates describing tools, cadences or roles the company does not use, so testing finds the written control and actual practice disagree.
CC2.2 Internal communication of responsibilities	PL-02 Publish policies where every employee and contractor can find them, have each person acknowledge them at hire and annually, and tell staff how to report a security concern or policy violation.	- Acknowledgment report showing each person, the policy version acknowledged and the date (Training platform) - Internal handbook page listing current policies and the channel for reporting security concerns (Policy repository) - Notice sent to staff when a policy changed materially, with the date sent (Policy repository)	Acknowledgments for everyone hired in the period and for the annual cycle, plus a staff notice for each material policy change made during the period.	Annual	A policy changed mid-period but staff only ever acknowledged the old version, or contractors with system access acknowledged nothing.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC2.3 Communication with outside parties	PL-03 Tell customers what you commit to and what they must do themselves: state security commitments in contracts or a trust page, publish a security contact, and notify customers of changes that affect them.	- Customer agreement or terms showing your security, availability and confidentiality commitments (Customer and vendor contracts) - Published security contact and vulnerability reporting route, such as a security page or security.txt file (Customer communications) - Customer documentation of the controls customers run themselves, such as managing their own users and SSO (Customer communications) - Dated notices to customers about material changes, such as new subprocessors or changed commitments (Customer communications)	Dated customer notices for changes made in the period, and a record that reports to the security contact were received and answered.	Per event	Customer responsibilities assumed in the system description are never communicated to customers, or the security contact goes to an unmonitored inbox.
CC1.4 Hiring and keeping competent people	HR-01 Run background checks, where local law allows, on employees and contractors who will have access to production or customer data, and complete each check before that access is granted.	- Background check completion records with the completion date for each in-scope hire (HR system) - Hiring procedure stating which roles are screened and what the check covers in each country (Policy repository)	A check completed before the access grant for every in-scope hire in the period, so the auditor can compare check dates with provisioning dates.	Per event	Checks finish after the person already has production access, or contractors and staff hired through agencies bypass the process.
CC1.4 Hiring and keeping competent people CC2.2 Internal communication of responsibilities	HR-02 Train every employee and contractor on security at hire and annually, and give engineers and support staff extra training on secure coding and handling customer data.	- Training completion report listing each person, the course and the completion date (Training platform) - Course content covering phishing, data handling, incident reporting and acceptable use (Training platform) - Role-specific completion records, such as secure coding training for engineers (Training platform)	Completion records for each new hire within the deadline your policy sets and for the annual cycle, covering everyone active during the period.	Annual	New hires finish training weeks after starting, or the completion report leaves out contractors and people who left during the period.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC1.5 Accountability for controls	HR-03 Review each employee's performance at least annually, including how they carry out assigned security responsibilities, and apply a documented disciplinary process when someone breaks a policy.	- Dated performance review records showing reviews were completed for current employees (HR system) - Disciplinary procedure referenced by the security policies (Policy repository) - Record of each policy violation in the period and the action taken (HR system)	Completed reviews for employees active through the review cycle, and a record for each policy violation found during the period.	Annual	Performance reviews at an early-stage company are informal conversations, so there is no dated record for the auditor to inspect.
CC3.1 Objectives clear enough to assess risk CC3.2 Risk identification and analysis	RA-01 Each year, write down your service commitments and security objectives, identify threats to them (including vendor risks), rate each risk's likelihood and impact, and record a treatment decision and owner for every risk.	- Statement of the service commitments and system requirements the assessment started from (Board and management records) - Dated risk register listing each risk, its rating, treatment decision, owner and linked controls (Risk register) - Management sign-off on the completed assessment and on any risks accepted rather than treated (Board and management records)	An assessment completed within the period on the cadence your policy states, with treatment actions tracked to completion or formally accepted.	Annual	The register is a template that never changes from year to year, or its risks are not linked to the controls meant to treat them.
CC3.3 Fraud risk	RA-02 Include fraud in the risk assessment: consider how staff, contractors or outsiders could misuse access, alter records or billing, or override controls, and name the controls that address each scenario.	- Fraud scenarios in the risk register with ratings and the controls that mitigate each (Risk register) - Assessment notes showing who considered insider misuse, management override and payment or billing fraud (Risk register)	The fraud portion of the assessment completed within the period, with any resulting actions tracked.	Annual	The risk assessment covers outside attackers only and never considers insider misuse or management overriding a control.
CC3.4 Significant changes	RA-03 Before a significant change, such as a new product line, a major architecture change, an acquisition or a new critical vendor, assess its effect on security risk and update the risk register and controls.	- Risk review ticket or note for each significant change, with the date and the decision (Ticketing system) - Risk register entries added or updated as a result of each review (Risk register)	A risk review for each significant change made during the period, dated before or at the change, so the auditor can match changes to reviews.	Per event	Major changes such as a new cloud region or an AI feature ship with no record that their risks were considered until the next annual assessment.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC5.1 Controls that reduce risk CC5.2 General technology controls CC1.5 Accountability for controls	RA-04 Maintain a control matrix that links each risk to the controls that treat it, including technology controls over infrastructure, access and software development, and names an owner and cadence for every control.	- Control matrix listing each control with its owner, cadence, the risks it addresses and the criteria it maps to (Risk register) - Record of the annual matrix review showing controls added, changed or retired (Board and management records)	The matrix in force during the period, and evidence that each named owner performed their control at the stated cadence.	Annual	A control has no owner, or the named owner left the company, so nobody performed it for part of the period.
CC4.1 Ongoing and separate evaluations	CE-01 Monitor whether each control ran on its cadence, using automated tests where available and a dated checklist where not, and have a named owner review the results at least monthly.	- Control monitoring log or dashboard export showing each control's test results and dates (Compliance platform) - Tickets opened for failed control tests, with owner and resolution date (Ticketing system)	Dated monitoring results across the whole period with no unexplained gaps, and follow-up recorded for each failure.	Monthly	A compliance platform shows tests failing for weeks with no ticket or owner response, so the monitoring control looks as if it did not operate.
CC4.1 Ongoing and separate evaluations	CE-02 Once a year, have someone independent of the control owners, such as an internal auditor or outside consultant, evaluate whether key controls are designed and operating as described. The SOC 2 audit itself does not count.	- Dated evaluation report naming the evaluator, the controls covered, the method used and the findings (Board and management records) - Management response to each finding with owner and due date (Ticketing system)	An evaluation performed within the period by someone who does not run the controls, with its findings entered in deficiency tracking.	Annual	The only evaluation is a self-assessment by the people who run the controls, or its scope skips the controls most likely to fail.
CC4.2 Reporting and fixing deficiencies	CE-03 Log every control failure, audit finding and test exception as a deficiency with an owner, severity and due date, report open items to management, and track each one to closure.	- Deficiency log or tickets with severity, owner, due date and closure evidence (Ticketing system) - Management or board report showing open deficiencies and their status (Board and management records)	Each deficiency raised during the period traced to remediation or a documented acceptance, with reports to management on the stated cadence.	Quarterly	Deficiencies get fixed with no record, or sit open past their due dates with no escalation to management.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC6.1 Logical access security	AC-01 Require multi-factor authentication for every workforce account on in-scope systems, through single sign-on where the system supports it, and turn off sign-in methods that bypass it, such as local passwords. Give each person a unique user ID, with no shared accounts.	- Identity provider policy export showing MFA required, not optional, for all users (Identity provider) - List of in-scope applications connected to SSO, with any exceptions and their compensating controls (Identity provider) - Settings for accounts outside SSO, such as the cloud root account, showing MFA enforced (Cloud console) - User list showing one named account per person and no shared logins (Identity provider)	Configuration evidence that enforcement stayed on through the period, and a record of each exception approved and when it ended.	Continuous	MFA is offered but not enforced, or root, break-glass (emergency admin) and non-SSO accounts still sign in with a password alone.
CC6.1 Logical access security	AC-02 Store secrets, API keys and service-account credentials in a secrets manager, give each service account a named owner, and rotate or revoke credentials when an owner leaves or a key is exposed.	- Secrets manager configuration and access policy showing who can read production secrets (Cloud console) - Service account inventory with owner, purpose and last rotation date (Cloud console) - Secret-scanning results for code repositories, with each detected secret revoked (Source control and CI/CD)	Rotation or revocation records for credentials owned by people who left, or for keys exposed, during the period.	Per event	Long-lived service account keys have no owner and were never rotated, or secrets sit in source code and committed configuration files.
CC6.2 User registration and removal	AC-03 Grant access to in-scope systems only after a recorded approval from the person's manager or the system owner, at the level the role needs. Apply this to employees, contractors and vendor users alike.	- Access request tickets showing requester, approver, systems, access level and approval time (Ticketing system) - Account creation timestamps to compare against each approval time (Identity provider) - Role-to-access mapping used to set default access for each job (Policy repository)	An approval dated before provisioning for each account created in the period, drawn from a complete list of new accounts.	Per event	Accounts are created before approval is recorded, or access is granted over chat and the ticket is written afterward.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC6.2 User registration and removal	AC-04 Remove all access for departing employees and contractors by the deadline in your access policy, triggered by the HR termination record, and recover company devices.	- Termination list showing each person's last day (HR system) - Account deactivation timestamps for the same people (Identity provider) - Offboarding tickets showing access removed from systems outside SSO and devices returned (Ticketing system)	For every person who left during the period, a deactivation time within the policy deadline of their termination date.	Per event	Accounts outside SSO, such as the cloud console, the database or a shared admin tool, stay active after the identity provider account is disabled.
CC6.3 Role-based access and least privilege CC5.2 General technology controls	AC-05 Define roles with the minimum permissions each job needs, assign access through those roles or groups rather than one-off grants, and require approval for anything beyond the role.	- Role matrix listing each role and the permissions it grants in each system (Policy repository) - Export of current user-to-role and group assignments (Identity provider) - Approval tickets for permissions granted outside a standard role (Ticketing system)	Approval records for role changes and extra permissions granted in the period, and assignments that still match the role matrix.	Per event	Most users hold an admin or owner role because it was easier, so the documented role matrix does not match real permissions.
CC6.2 User registration and removal CC6.3 Role-based access and least privilege	AC-06 Each quarter, have system owners review every account and its permissions on production and other in-scope systems, record a keep or remove decision for each, and remove unneeded access by a set deadline.	- Dated export of the accounts and permissions used for each review (Identity provider) - Quarterly access review sign-off listing the reviewer, the accounts reviewed, the decisions and the changes made (Ticketing system) - Removal records showing access marked for removal was actually removed (Ticketing system)	A completed review for every quarter in the period, each with the population reviewed, the decisions made and proof that removals happened.	Quarterly	Reviewers approve the whole list without checking actual permissions, or removals decided in the review are never carried out.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC6.1 Logical access security CC6.3 Role-based access and least privilege	AC-07 Limit admin and production data access to named people with a recorded need, use separate or time-limited elevated sessions for admin work, keep a monitored break-glass (emergency admin) account, and log privileged actions.	- List of admin and production-access accounts with the justification for each (Cloud console) - Access settings showing elevated rights are time-limited or need a separate role (Cloud console) - Break-glass procedure stating who holds the credentials and when the account may be used (Policy repository) - Admin activity log tying privileged actions to named people, including each break-glass use and its review (Logging and monitoring (SIEM))	Privileged access lists reviewed through the period, and a log entry and review for each break-glass use.	Quarterly	Shared admin credentials or the cloud root account are used for routine work, so actions cannot be tied to a person.
CC6.1 Logical access security	AC-08 Protect customer logins to your product: enforce password rules, offer MFA or SSO, throttle repeated failed attempts, expire idle sessions, and check tenant boundaries on every data request.	- Application authentication settings or code showing password rules, logout and session timeouts (Application and data stores) - Automated tests or code review records covering tenant isolation on data queries (Source control and CI/CD) - Penetration test results covering authentication and cross-tenant access (Penetration test or external assessment)	Code or configuration history showing the settings stayed in place through the period, and test results that cover the release in use.	Continuous	Tenant isolation is enforced only in the user interface, so a signed-in user can fetch another customer's records through the API.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC6.1 Logical access security CC6.6 Protection against outside threats	AC-09 Each quarter, review the third-party apps and OAuth grants connected to your workspace, code host and chat tools, remove any that are unused or unapproved, and limit who can authorize new ones.	- Export of connected apps and OAuth grants with their scopes and the user who authorized each (Identity provider) - List of apps and integrations installed in the code host, with their permissions (Source control and CI/CD) - Admin setting restricting which users may approve new third-party apps (Identity provider) - Review record listing the apps removed and the date (Ticketing system)	A completed review for each quarter in the period, with the removals it decided carried out.	Quarterly	Old integrations keep broad access to email, files or repositories long after the person who connected them has left.
CC6.4 Physical access	PE-01 Restrict entry to offices and to any room holding network or storage equipment to authorized people, log visitors, and remove badge or key access when people leave.	- Badge system user list compared with current staff, or a key issuance log (Physical security records) - Visitor log for the period (Physical security records) - Badge or key removal records for departed staff (Physical security records)	Visitor entries and badge removals across the period, with each departure matched to a badge deactivation.	Per event	Badges stay active after people leave, or a shared office has no record of who can enter.
CC6.4 Physical access A1.2 Environmental protection, backup and recovery	PE-02 As part of the vendor review, read your cloud and hosting providers' SOC 2 reports each year for their physical and environmental protection results, note any exceptions, and confirm you perform the controls they expect of customers.	- Current SOC 2 report for each hosting provider, with the period it covers (Vendor inventory) - Review note recording physical and environmental protection results, exceptions and the customer controls you rely on (Vendor inventory)	A review done during the period of a report whose coverage overlaps your period, with a bridge letter (the provider's statement covering the months since its report ended) on file for any gap.	Annual	The provider's report is downloaded but never read, so its exceptions and the customer controls it expects go unaddressed.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC2.1 Quality information for controls CC6.1 Logical access security	AM-01 Maintain an inventory of in-scope systems, cloud accounts, SaaS tools, data stores and company devices with an owner for each, plus a current network and data-flow diagram.	- System and data store inventory with owner, environment and data classification (Asset inventory) - Cloud resource export used to confirm the inventory is complete (Cloud console) - Network and data-flow diagrams with a revision date (Policy repository) - Device inventory with assigned user and serial number (Asset inventory)	Inventory updates for systems and devices added or retired during the period, and diagrams that match the environment as it ran.	Quarterly	Resources created during the period, such as a new database or cloud account, never reach the inventory and so miss logging, backups and reviews.
CC6.5 Asset disposal C1.2 Disposing of confidential information	AM-02 Before a device or storage medium is reused, returned or thrown away, wipe or destroy it by a method suited to the data it held, and record the asset, method, date and who did it.	- Disposal log linked to the asset inventory, with method, date and the person who performed it (Asset inventory) - Remote wipe confirmation for each managed device (Endpoint management (MDM)) - Destruction certificate from the disposal vendor listing serial numbers (Asset inventory)	A disposal record for every device retired during the period, traceable to its inventory entry.	Per event	Laptops from departed staff are reissued or sold without a recorded wipe, or the destruction certificate lists no serial numbers.
CC6.6 Protection against outside threats	NS-01 Expose to the internet only the endpoints the service needs, keep admin interfaces and databases off public networks, segment internal networks so production is separate, use provider protections such as a web firewall or rate limits, and review exposure rules each quarter.	- Firewall, security group or platform network settings showing the inbound traffic allowed (Cloud console) - Network layout showing production separated from other environments and internal services (Cloud console) - Inventory of public endpoints and domains with an owner for each (Asset inventory) - Dated quarterly review of inbound rules with the changes made (Ticketing system)	Rule reviews on the stated cadence, and change records for exposure rules altered during the period.	Quarterly	Broad inbound rules, such as an open database port, were added for testing and never removed, or production shares a flat network with everything else.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC6.6 Protection against outside threats CC6.1 Logical access security	NS-02 Reach production servers and networks only through an authenticated, logged path such as a bastion host (a hardened jump server), VPN, zero-trust proxy or the cloud provider's session manager, never through SSH or RDP exposed to the internet.	- Remote-access path configuration showing SSO and MFA required (Cloud console) - Session logs for production connections made through that path (Logging and monitoring (SIEM)) - Network rules showing SSH and RDP closed to the internet (Cloud console)	Session logs across the period showing production access went through the approved path.	Continuous	SSH is open to the internet with shared keys, so production access is neither tied to a person nor logged.
CC6.7 Data transmission and removal	NS-03 Encrypt data in transit on every external connection with TLS 1.2 or later, turn off older protocols, and let customer data leave production only through approved transfer methods that leave a record.	- TLS scan results for public endpoints showing the protocol versions accepted (Vulnerability scanner) - Data handling rule naming approved transfer methods and barring personal email or storage for customer data (Policy repository) - Log or tickets for bulk exports of customer data (Application and data stores)	Scan results across the period showing TLS settings held, and a record for each bulk export of customer data.	Continuous	A legacy endpoint still accepts TLS 1.0, or engineers export customer data to laptops and spreadsheets with no record.
CC6.1 Logical access security CC6.8 Malicious software	EP-01 Enroll every company laptop in device management and enforce disk encryption, screen lock, automatic OS updates and remote wipe, with alerts when a device falls out of compliance.	- Enrollment report compared with the device inventory (Endpoint management (MDM)) - Compliance report showing encryption, screen lock and OS version for each device (Endpoint management (MDM)) - Tickets for non-compliant devices with the fix and the date (Ticketing system)	Compliance reports from across the period, not only its end, and a resolution record for each device that fell out of compliance.	Continuous	Contractors' laptops are never enrolled, or non-compliant devices stay that way for months because nobody acts on the alerts.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC6.8 Malicious software	EP-02 Run malware protection on laptops and on servers where the platform allows it, restrict or monitor software installation on company devices, and investigate and close every malware alert.	- Endpoint protection coverage report listing devices, agent status and last check-in (Endpoint management (MDM)) - Malware alert log with the investigation and outcome for each alert (Logging and monitoring (SIEM)) - Device settings or reports that restrict or monitor software installation and local admin rights (Endpoint management (MDM))	Coverage reports across the period and a closed record for every malware alert raised.	Continuous	Some devices never installed the agent or stopped reporting, unnoticed because coverage was never compared with the inventory.
CC6.1 Logical access security CC6.8 Malicious software	EP-03 Set a minimum baseline for any device that reaches company systems, including personal ones: disk encryption, screen lock, a supported OS and malware protection. Check it with device posture rules or signed attestations.	- Device security standard stating the baseline and which devices it covers (Policy repository) - Device posture rules in the identity provider blocking devices that miss the baseline (Identity provider) - Dated signed attestation from each person using a personal device (Compliance platform)	Posture checks or attestations covering everyone who used an unmanaged device during the period, on the cadence your standard sets.	Quarterly	Personal devices are allowed but the policy says nothing about them, so the auditor finds devices with no proof of encryption or updates.
CC7.1 Configuration and vulnerability detection	VM-01 Set secure configuration baselines for cloud accounts and hosts or containers, or for your managed platform's security settings. Scan for vulnerabilities, misconfigurations and outdated dependencies on a set schedule and after major changes, across every in-scope environment.	- Configuration baseline or hardening standard, including the security settings of any managed platform (Policy repository) - Dated scan reports from across the period with the assets each scan covered (Vulnerability scanner) - Configuration findings measured against the baseline (Cloud console) - Dependency scanning results from the CI pipeline (Source control and CI/CD)	A dated scan for every scheduled interval in the period, with coverage that matches the system inventory.	Monthly	Scans cover only part of the environment, such as one cloud account, or the schedule lapsed for a month with no record of why.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC7.1 Configuration and vulnerability detection	VM-02 Fix vulnerabilities and apply security patches within deadlines set by severity in your policy, track each finding in a ticket, and record a signed risk acceptance for anything that cannot meet its deadline.	- Remediation tickets for critical and high findings with open date, owner and close date (Ticketing system) - Follow-up scan showing each fixed finding cleared (Vulnerability scanner) - Signed risk acceptances for findings left open past their deadline (Risk register)	For findings raised in the period, close dates within the policy deadline or an approved acceptance, which the auditor can sample against scan output.	Per event	The same critical finding appears in several months of scans with no ticket and no recorded risk acceptance.
CC4.1 Ongoing and separate evaluations CC7.1 Configuration and vulnerability detection	VM-03 Commission an independent penetration test of the in-scope application and infrastructure at least annually and after major changes, then fix the findings and retest the serious ones.	- Penetration test report with scope, dates, tester, method and findings (Penetration test or external assessment) - Remediation tickets for each finding, closed or formally accepted (Ticketing system) - Retest report or letter confirming high-severity fixes (Penetration test or external assessment)	A test dated within the period, or recent enough for your auditor to accept it, scoped to the system as it ran, with findings tracked to closure.	Annual	The test scope leaves out the production application or its API, or findings are filed with no remediation record or retest.
CC7.2 Monitoring for anomalies CC2.1 Quality information for controls	LG-01 Send security-relevant logs from the cloud, identity provider, application and other in-scope systems to a central store, protect them from change, and keep them long enough that the start of the audit period is still available when the auditor tests it.	- Logging configuration showing audit logs enabled in every cloud account and region in use (Cloud console) - List of log sources feeding the central store, compared with the system inventory (Logging and monitoring (SIEM)) - Retention and access settings for the log store (Logging and monitoring (SIEM))	Logs available for the full period, so the auditor can pull events from its first months as well as its last.	Continuous	A cloud account or service added during the period was never connected to logging, or retention deletes the period's first months before fieldwork.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC7.2 Monitoring for anomalies CC7.3 Evaluating security events	LG-02 Alert on suspicious activity such as repeated failed logins, privilege changes and unusual data access, route alerts to an on-call owner, and record a triage decision for each against written severity criteria.	- Alert rule configuration listing what triggers each alert and where it is sent (Logging and monitoring (SIEM)) - On-call schedule or alert routing in effect during the period (Logging and monitoring (SIEM)) - Alert records with acknowledgment time, triage notes and outcome (Ticketing system) - Severity criteria for deciding when an event is an incident (Policy repository)	A triage record for alerts raised throughout the period, showing who reviewed each one and whether it became an incident.	Continuous	Alerts land in a chat channel nobody owns, so there is no record that anyone looked at them or decided whether they were incidents.
CC7.4 Incident response	IR-01 Keep an incident response plan that defines severity levels, roles, escalation, containment, evidence preservation, and customer and regulator communications, and review it at least annually.	- Incident response plan with owner, version and last review date (Policy repository) - Current contact list for responders, legal counsel and critical vendors (Policy repository)	The plan reviewed within the period, and incidents in the period handled according to its steps.	Annual	The plan names people who have left or tools the company no longer uses, so it has not been kept current.
CC7.4 Incident response CC7.5 Incident recovery	IR-02 Test the incident response plan at least once a year with a tabletop exercise or simulation that includes recovery steps, then update the plan with what the exercise showed.	- Exercise record with date, scenario, participants and findings (Exercise and test records) - Tickets or plan revisions made from the exercise findings (Ticketing system)	An exercise dated within the period, with its follow-up actions completed or tracked.	Annual	The plan was never exercised, or a tabletop happened but nothing records who took part or what changed afterward.
CC7.4 Incident response CC7.5 Incident recovery	IR-03 Record every security incident with its timeline, the actions taken, the systems restored and how their integrity was confirmed, and complete a post-incident review with corrective actions for significant incidents.	- Incident tickets with detection, containment, recovery and closure times (Ticketing system) - Post-incident reviews with root cause and corrective actions (Ticketing system) - Corrective action tickets tracked to completion (Ticketing system)	A complete incident log for the period with full records for each sampled incident. If none occurred, the auditor may rely on the exercise instead.	Per event	Incidents were handled in chat with no ticket, so nothing shows the response or recovery, or corrective actions were never finished.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC2.3 Communication with outside parties CC7.4 Incident response	IR-04 Notify affected customers, and regulators where required, about security incidents within the time frames set by your contracts and applicable law, and keep a copy of each notice.	- Notification procedure listing the contractual and legal notice deadlines that apply (Policy repository) - Copies of notices sent, with dates, to compare against the incident timeline (Customer communications) - Customer contract clauses setting notification commitments (Customer and vendor contracts)	A dated notice for each incident in the period that required one, sent within the committed deadline.	Per event	Contracts promise notice within a set number of hours that the incident plan never mentions, so nobody tracks that deadline.
CC8.1 Change management CC5.1 Controls that reduce risk	CM-01 Require a pull request reviewed and approved by someone other than the author before any code or infrastructure-as-code change merges to the production branch, enforced by branch protection.	- Branch protection settings requiring approval and blocking self-approval and force pushes (Source control and CI/CD) - List of pull requests merged during the period with reviewer and approval time (Source control and CI/CD) - List of who can bypass branch protection, and a log of each bypass (Source control and CI/CD)	Branch protection on throughout the period, and an approval from someone other than the author on each sampled merge.	Per event	Admins can bypass branch protection and did, or infrastructure is changed in the cloud console instead of through reviewed code.
CC8.1 Change management	CM-02 Run automated tests and security checks in the CI pipeline on every change, and block the merge or deploy when they fail.	- CI configuration showing the checks required on the production branch (Source control and CI/CD) - Pipeline run history showing checks passed for each deployed change (Source control and CI/CD)	Passing check results tied to the changes deployed during the period.	Per event	Tests run but are not required, so changes merge with failing or skipped checks.
CC8.1 Change management CC5.2 General technology controls	CM-03 Deploy to production only through the pipeline from the approved branch, restrict who can change production directly, and record each deployment with its commit and time.	- Deployment log linking each release to a commit, an approved change and a timestamp (Source control and CI/CD) - List of people with direct write access to production, with the reason for each (Cloud console)	A deployment record for every release in the period that ties back to an approved change.	Per event	Engineers deploy from their laptops or edit production directly, leaving changes with no review or record.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC8.1 Change management	CM-04 Define an emergency change path that lets an urgent fix ship first, then requires review, test evidence and approval within a set number of business days.	- Emergency change procedure stating who can use it and the follow-up deadline (Policy repository) - Emergency change tickets with after-the-fact review and approval dates (Ticketing system)	Each emergency change in the period identified as one and approved after the fact within the deadline.	Per event	Hotfixes go straight to production with no ticket and no later review, and nobody can list which changes were emergencies.
CC8.1 Change management C1.1 Identifying and protecting confidential information	CM-05 Keep development and test environments separate from production, and keep real customer data out of them unless it is masked or the copy is approved.	- Cloud account or project structure showing separate production and non-production environments (Cloud console) - Test data rule and the approval for each copy of production data made (Policy repository)	No unapproved production data in lower environments during the period, and an approval and masking record for each copy made.	Continuous	A production database snapshot was restored to staging for debugging and left there under weaker access controls.
CC8.1 Change management	CM-06 Make manual changes to production data, such as fixes run as scripts or edits in a database console, only through an approved ticket, and keep a record of exactly what was run.	- Tickets for production data changes with the approval and the script or query run (Ticketing system) - Database audit log of changes made outside the application (Logging and monitoring (SIEM))	An approved ticket for each manual data change in the period that matches the database log.	Per event	Support engineers fix customer records directly in the database with no ticket, so the changes cannot be matched to an approval.
CC9.2 Vendor and business partner risk	VR-01 Keep an inventory of vendors that hold or can reach customer data or affect the service, with a risk tier, an owner and the data each receives. Update it as vendors change, and revoke access when one leaves.	- Vendor inventory with risk tier, owner, data shared and contract dates (Vendor inventory) - Offboarding records for vendors removed in the period, showing access revoked and data returned or deleted (Vendor inventory)	Inventory updates for vendors added and removed during the period, each traceable to a contract or invoice.	Per event	Tools bought on a company card or by a single team never reach the inventory, so they skip review entirely.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC9.2 Vendor and business partner risk	VR-02 Assess each vendor's security before signing, and yearly for high-risk ones. Review the SOC 2 report of every provider your service runs on; where none exists, record what you checked instead and a risk decision. Note exceptions and the controls each vendor expects of you.	• Vendor review records with date, reviewer, report period covered and conclusion (Vendor inventory) • Current SOC 2 report for each provider the service runs on, or a record of what was checked instead and the risk decision (Vendor inventory) • List of controls each key vendor expects you to run, and how you meet them (Vendor inventory)	A review before onboarding for each vendor added in the period, and an annual review for each high-risk vendor.	Annual	Vendors are signed before security reviews them, or a critical provider has no SOC 2 report and nothing records what was checked instead.
CC9.2 Vendor and business partner risk CC2.3 Communication with outside parties	VR-03 Include security, confidentiality, breach notification and data return or deletion terms in contracts with vendors that handle customer data or affect the service.	• Signed agreements or data processing addenda with security and breach-notice clauses (Customer and vendor contracts) • Contract checklist or template listing the terms required for each vendor tier (Customer and vendor contracts)	Signed terms in place, before they received customer data, for vendors added during the period.	Per event	Click-through terms with key vendors were never checked, so there is no breach-notice commitment the company can rely on.
A1.2 Environmental protection, backup and recovery CC9.1 Business disruption risk	BC-01 Back up production databases and other critical data automatically, encrypt the backups, store them apart from the primary system, and alert an owner when a backup fails.	• Backup configuration showing schedule, retention, encryption and storage location (Backup system) • Backup job history across the period, with failures and their follow-up (Backup system)	Backup job results across the period, with each failure investigated and resolved.	Continuous	A database added mid-period was never added to the backup schedule, or failure alerts go to no one.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC9.1 Business disruption risk CC1.4 Hiring and keeping competent people	BC-05 Keep a business continuity plan that covers losing key people, vendors, offices or systems, cross-train or name a successor for each critical role, decide which risks to transfer through insurance, and review the plan annually.	• Business continuity plan with owner and last review date (Policy repository) • Business impact analysis listing critical processes and their dependencies (Risk register) • Cross-training or succession record naming a backup for each critical role (HR system) • Cyber insurance policy, or the documented decision not to carry one (Customer and vendor contracts)	The plan and impact analysis reviewed within the period.	Annual	The plan covers a data center outage but not losing the one engineer who knows how to deploy, or an outage at a critical vendor.
CC6.1 Logical access security C1.1 Identifying and protecting confidential information	DP-01 Encrypt customer data at rest in databases, storage, backups and replicas, manage keys in your provider's key management service, and limit who can use or change the keys.	• Encryption-at-rest settings for each data store, backup and replica (Cloud console) • Key policies showing who can use and who can administer each key (Cloud console)	Encryption on for data stores created during the period, not only for those that existed at the start.	Continuous	A storage bucket or replica created mid-period was left unencrypted, and the gap surfaces when the inventory is compared with a live export.
CC9.2 Vendor and business partner risk	AIM-01 Approve each hosted AI model provider and AI tool before customer data is sent to it, review its security, data use and retention terms, keep an approved list staff must follow, and list providers that receive customer data as subprocessors.	• Approved list of AI providers and tools with the data types permitted in each (Vendor inventory) • Security review for each AI provider covering its assurance reports and data terms (Vendor inventory) • Acceptable-use rule for AI tools, acknowledged by staff (Policy repository) • Subprocessor list entries for each AI provider that receives customer data (Customer communications)	A review dated before first use for each AI provider or tool added during the period.	Per event	Staff paste customer data into AI tools nobody approved, so the vendor inventory misses providers that now hold customer data.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
CC6.7 Data transmission and removal C1.1 Identifying and protecting confidential information	AIM-02 Configure each AI provider so customer data is not used for training, retention is the shortest available and data stays in committed regions. Redact or allowlist the fields sent to models. Recheck quarterly and when terms change.	- Provider account settings showing training opt-out, retention period and data region (AI model provider console) - Provider data terms or enterprise agreement confirming training and retention commitments (Customer and vendor contracts) - Data-flow diagram showing which customer data is sent to each model (Policy repository) - Redaction rules or field allowlist applied before requests reach a model (Source control and CI/CD)	Settings evidence from within the period, and a recorded check each time the provider changed its terms.	Quarterly	A developer account on default terms runs in production, so prompts may be retained or used for training against customer commitments.
CC7.2 Monitoring for anomalies	AIM-03 Log AI requests made by the product with timestamp, model and version, the calling user or service, and any tool actions taken. Store prompt content only where needed, and restrict access to logs that contain customer data.	- Logging configuration for AI calls showing the fields captured (Logging and monitoring (SIEM)) - Sample log entries tying requests to users and model versions (Logging and monitoring (SIEM)) - Retention and access settings for logs holding prompts or outputs (Logging and monitoring (SIEM))	AI request logs available across the period at the level of detail your control describes.	Continuous	Raw prompts containing customer data are kept indefinitely in a general log store that most of the company can read.
CC8.1 Change management	AIM-04 Treat changes to prompts, model versions, retrieval sources and AI tool permissions as production changes: review, test against an evaluation set, approve and record each one.	- Pull requests or tickets for prompt and model changes, with approval (Source control and CI/CD) - Evaluation results run before each release (Source control and CI/CD) - Version history of prompts and model configuration (Source control and CI/CD)	A review and evaluation record for each AI change released during the period.	Per event	Prompts are edited in a provider dashboard outside source control, so changes have no review, test or history.

Availability controls (A1.1–A1.3)

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
A1.2 Environmental protection, backup and recovery	BC-02 Document a disaster recovery plan with recovery time and recovery point targets that match customer commitments, and design production so it can meet them, for example with multi-zone deployment or a tested restore path.	- Disaster recovery plan with recovery time and recovery point targets, roles and recovery steps (Policy repository) - Architecture settings or restore design showing how the targets can be met, such as multi-zone deployment (Cloud console)	The plan reviewed within the period, and a production design that matched it while the service ran.	Annual	Recovery targets in customer contracts are tighter than anything the architecture or backup schedule could deliver.
A1.3 Recovery plan testing	BC-03 Test recovery at least annually by restoring backups and walking through the disaster recovery plan, compare the results with recovery targets, and fix the gaps found.	- Restore test record with date, data restored, time taken and how the result was validated (Backup system) - Recovery test report comparing results with recovery targets, with lessons learned (Exercise and test records) - Tickets for gaps found in testing (Ticketing system)	A recovery test dated within the period, with results recorded and follow-up completed.	Annual	Backups run every day but nobody has ever restored one, so the plan's recovery times are untested assumptions.
A1.1 Capacity monitoring	BC-04 Monitor use of compute, storage and database capacity against set thresholds, alert before limits are reached, and review capacity needs on a set cadence.	- Monitoring dashboards and alert thresholds for capacity metrics (Logging and monitoring (SIEM)) - Capacity review notes or tickets with the actions taken (Ticketing system)	Capacity alerts and reviews across the period, with the actions taken for each.	Quarterly	Dashboards exist but no thresholds are defined, so nobody is alerted until customers notice slowdowns.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
A1.1 Capacity monitoring CC7.2 Monitoring for anomalies CC2.3 Communication with outside parties	BC-06 Monitor availability with external uptime checks, handle outages through the incident process, keep customers informed on a status page, and measure availability against the targets you commit to. The trust services criteria set no uptime number; your commitments do.	• Uptime monitor setup showing the endpoints checked, the interval and where alerts go (Logging and monitoring (SIEM)) • Outage tickets with start and end times, cause and customer impact (Ticketing system) • Status page history showing outage notices and updates (Customer communications) • Availability measured for each reporting interval and compared with customer commitments (Logging and monitoring (SIEM))	Uptime data for the whole period, an outage record and status update for each outage, and availability compared with commitments for each interval.	Continuous	Contracts promise an uptime percentage that nobody measures, or outages were fixed with no status update and no record of how long they lasted.

Processing Integrity controls (PI1.1–PI1.5)

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
PI1.1 Processing specifications	PRC-01 Document each in-scope process: the inputs it accepts, what it does to them, the outputs it produces, and the accuracy and timing you promise customers.	• Processing specifications or data dictionary for each in-scope workflow (Application and data stores) • Customer documentation describing processing commitments (Customer communications)	Specifications updated for each processing change released during the period.	Annual	Processing logic lives only in code and in engineers' heads, so the auditor has nothing to test the outputs against.
PI1.2 Input controls	PRC-02 Validate inputs on the server for type, format, range and required fields, reject or hold bad records, and log each rejection so it can be corrected.	• Validation rules in code or configuration (Source control and CI/CD) • Rejected-input logs or error queues with how each record was resolved (Application and data stores)	Rejection logs across the period, and evidence that rejected records were corrected or returned.	Continuous	Validation runs only in the browser, so API callers can submit records that skip it.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
PI1.3 Processing controls	PRC-03 Monitor processing jobs for failures, delays and incomplete runs, alert an owner, and record how each exception was fixed or the data reprocessed.	- Job monitoring dashboard and alert settings (Logging and monitoring (SIEM)) - Exception tickets showing cause, reprocessing and resolution (Ticketing system)	Exceptions raised during the period, each with a resolution record.	Continuous	Failed jobs retry silently or drop records, and nobody can show that every input was processed.
PI1.3 Processing controls	PRC-04 Test every change to processing logic, such as calculations and data transformations, against expected results before release, hotfixes included.	- Test cases for processing logic with their expected results (Source control and CI/CD) - Release records showing those tests passed before deployment (Source control and CI/CD)	Passing test results for each processing change released during the period.	Per event	Hotfixes to processing logic skip the test suite, so calculation errors can reach customers.
PI1.4 Output controls	PRC-05 Reconcile outputs to inputs using record counts or control totals, and deliver outputs only to the intended recipients through approved channels.	- Reconciliation reports with any differences and their resolution (Application and data stores) - Output delivery settings showing recipients and access restrictions (Application and data stores)	A reconciliation for each processing run or batch in the period, with differences resolved.	Per event	Output reports are checked for format but never reconciled to inputs, so missing records go unnoticed.
PI1.5 Storage of inputs, work in progress and outputs	PRC-06 Protect stored inputs, in-process data and outputs from unauthorized change, keep an audit trail of changes to those records, and retain them as long as your specifications require.	- Audit trail or change history settings for in-scope records (Application and data stores) - Access settings limiting who can modify stored processing data (Cloud console) - Retention settings for inputs and outputs (Application and data stores)	Audit trail entries across the period showing changes were captured and attributable to a person or process.	Continuous	Records can be edited with no history, so nobody can show that stored outputs still match what was originally produced.

Confidentiality controls (C1.1–C1.2)

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
----------	---------	---------------------------	---	---------	------------

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
C1.1 Identifying and protecting confidential information	DP-02 Classify your data, mark which customer and business information is confidential, and set handling rules for each class covering where it may be stored, who may access it and how it may be shared.	- Data classification policy with handling rules for each class (Policy repository) - Data inventory showing where confidential information is stored and how it is classified (Asset inventory) - Customer contract clauses identifying information you must treat as confidential (Customer and vendor contracts)	Handling rules applied to data stores added during the period, with the inventory updated to match.	Annual	There is no classification scheme, so nobody can say which data the confidentiality terms in customer contracts actually cover.
C1.2 Disposing of confidential information	DP-03 Delete confidential information when its retention period ends or a customer leaves, including copies in exports and with vendors, let backups expire on schedule, and record each deletion.	- Retention schedule by data type, including backup expiry (Policy repository) - Deletion records or job logs for departed customers and expired data (Application and data stores) - Vendor confirmations of deletion where a vendor held the data (Vendor inventory)	A deletion record for each customer that left during the period, and logs from scheduled deletion jobs across it.	Per event	Deletion is promised in contracts but never done, or done in the main database while copies remain in exports and analytics tools.

Privacy controls (P1–P8 series)

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
P1.1 Privacy notice	PV-01 Publish a privacy notice covering what personal information you collect, why, how long you keep it, who receives it and people's rights, and update it before practices change. For data you process for customers, describe your handling in your terms or processing agreement.	- Current privacy notice with version history and effective dates (Privacy records) - Review record comparing the notice with actual data flows (Privacy records)	The notice versions in effect during the period, and a review showing they matched practice.	Annual	The notice was copied from a template and lists uses or retention periods that do not match what the product does.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
P2.1 Choice and consent P3.2 Explicit consent at collection	PV-02 Show people their choices when you collect personal information, record consent where law or your notice requires it (explicit for sensitive data), and honor withdrawals by the deadline your notice or the law sets.	- Consent records showing the person, what they agreed to, the notice version and a timestamp (Privacy records) - Opt-out and withdrawal requests with the date each took effect (Privacy records) - Screenshots of the consent and choice points in the product (Application and data stores)	Consent records for people who signed up during the period and the processing date for each withdrawal. For personal information customers send you, document that consent is their responsibility and process it only as your contract allows.	Per event	Consent is captured but stored without a timestamp or notice version, so the company cannot show what a person agreed to.
P3.1 Collection limited to stated objectives P4.1 Use limited to identified purposes	PV-03 Keep an inventory of the personal information you hold, each field's purpose and where it flows, and review new features before they collect it or use it for a new purpose. Use personal information customers send you only for the purposes in your contract with them.	- Personal data inventory or record of processing with the purpose for each category (Privacy records) - Privacy review records for new features and new data uses (Privacy records)	A privacy review for each feature launched during the period that touched personal information.	Per event	Analytics and support tools collect fields the notice never mentions, so collection goes beyond the stated purposes.
P4.2 Retention P4.3 Disposal	PV-04 Set retention periods for personal information, delete or anonymize it when the period ends or a valid deletion request arrives, and record each deletion.	- Retention schedule for each type of personal information (Privacy records) - Deletion job logs and deletion request records with completion dates (Application and data stores)	Deletion records for requests received and scheduled purges run during the period.	Per event	No retention periods are defined, so personal information is kept indefinitely across databases, logs and backups.
P5.1 Data subject access	PV-05 Handle requests from individuals to see their personal information: verify identity, respond within legal and committed deadlines, and log each request and response. Route requests about data you hold for a customer to that customer.	- Request log with received date, identity check, response date and outcome (Privacy records) - Request handling procedure, including when requests pass to the customer who controls the data (Policy repository)	A log entry and a response for each access request received during the period.	Per event	Requests arrive by email and are answered ad hoc with no log, so neither timeliness nor identity checks can be shown.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
P5.2 Correction requests P7.1 Data quality	PV-06 Let individuals correct their personal information, validate key fields when they are collected, pass corrections on to vendors that received the data, and route requests about customer-held data to that customer.	- Correction request log with outcome and date (Privacy records) - Product settings or support workflow that lets users update their own data (Application and data stores) - Validation rules that check key personal fields, such as email and date of birth, when they are collected (Source control and CI/CD)	A record for each correction request received in the period, including updates sent to vendors.	Per event	Corrections update the main database but not the copies held by vendors or downstream systems.
P6.1 Consent before disclosure to third parties P6.2 Record of authorized disclosures P6.7 Accounting of disclosures	PV-07 Share personal information with third parties only for purposes your notice describes or with consent, keep a list of subprocessors, and record disclosures so you can tell a person who received their data.	- Published subprocessor list with its change history (Customer communications) - Disclosure log for sharing outside the subprocessor list, such as legal requests (Privacy records) - Responses to individuals who asked who received their data (Privacy records)	Disclosure records for the period, and a notice for each subprocessor change made during it.	Per event	New subprocessors are added without updating the public list or notifying customers as their contracts require.
P6.3 Record of unauthorized disclosures P6.6 Breach notification to affected parties	PV-08 Log every unauthorized disclosure of personal information and assess whether notice is required. Where a customer controls the data, notify that customer, who notifies individuals and regulators. Where you control it, notify them yourself. Meet legal and contractual deadlines.	- Privacy incident log with date, data involved, assessment and notice decision (Privacy records) - Copies of notifications sent, with dates (Customer communications)	An entry for each privacy incident in the period, with its notice decision and any notices sent on time.	Per event	Small disclosures, such as an email sent to the wrong customer, are never logged, so the record of unauthorized disclosures is empty.

Criteria	Control	Evidence auditors request	Type 2: what must exist across the audit period	Cadence	Common gap
P6.4 Vendor privacy commitments P6.5 Vendor notice of unauthorized disclosures	PV-09 Sign data processing terms with every vendor that receives personal information, requiring privacy commitments that match yours and prompt notice of any unauthorized disclosure.	- Signed data processing agreements for each vendor that receives personal information (Customer and vendor contracts) - Vendor review notes on each vendor's privacy practices (Vendor inventory) - Disclosure notices received from vendors and how each was handled (Privacy records)	Agreements in place before personal information went to any vendor added during the period.	Per event	The vendor list and the signed processing agreements do not match, leaving some vendors with personal data and no privacy terms.
P8.1 Inquiries, complaints and monitoring	PV-10 Give individuals a way to send privacy questions and complaints, log and resolve each one, forward complaints about customer-controlled data to that customer, and review privacy compliance at least annually with fixes tracked.	- Privacy contact channel published in the notice (Customer communications) - Inquiry and complaint log with resolution dates (Privacy records) - Annual privacy compliance review with findings and remediation (Privacy records)	A logged outcome for each inquiry received in the period, and the annual review completed with follow-up.	Annual	Complaints reach support as ordinary tickets and are never flagged as privacy issues, so nobody reviews them for patterns or fixes the cause.