PCC LEARNING CENTER

Third-Party and Vendor Access Review Checklist

Find persistent access, unclear ownership, and avoidable vendor risk

Use this fillable worksheet to inventory vendor access, verify ongoing business need, review technical and contractual safeguards, and remove access cleanly when a relationship changes or ends.

Access is broader than a user account

- Include integrations, API keys, service accounts, certificates, and unattended remote tools.
- Include physical access, vendor-managed devices, shared credentials, and subcontractors.
- Treat 'we are not sure' as an inventory gap requiring an owner and deadline.

ORGANIZATION

REVIEW OWNER

REVIEW DATE

NEXT REVIEW DATE

Review aid only: confirm contract, privacy, employment, monitoring, retention, and regulatory obligations with qualified advisers.

Third-Party Access Inventory and Triage

Start with known vendors, then search identity, remote-access, firewall, application, finance, facilities, procurement, and contract records for access that may be missing.

VENDOR / SERVICE	OWNER	SYSTEM / DATA	ACCESS TYPE	REVIEW DATE	RISK

INVENTORY GAPS, UNKNOWN ACCESS, OR IMMEDIATE CONCERNS

Detailed Vendor Profile A

Document access from the business perspective and verify it against technical evidence. A signed contract alone does not prove current access is appropriate.

VENDOR / THIRD PARTY

INTERNAL BUSINESS OWNER

CONTRACT START / END

NEXT ACCESS REVIEW

RISK RATING / RATIONALE

BUSINESS PURPOSE AND SERVICES PROVIDED

PEOPLE, ACCOUNTS, ROLES, AND PRIVILEGED ACCESS

SYSTEMS, APPLICATIONS, NETWORKS, LOCATIONS, AND PHYSICAL ACCESS

DATA ACCESSED, STORED, TRANSFERRED, OR CREATED

REMOTE-ACCESS METHOD, MFA, LOGGING, AND MONITORING

TOKENS, API KEYS, CERTIFICATES, INTEGRATIONS, AND SERVICE ACCOUNTS

SUBCONTRACTORS, DATA LOCATION, RETENTION, RETURN, AND DELETION

INCIDENT CONTACT, NOTIFICATION PERIOD, INSURANCE, AND CONTINUITY EVIDENCE

Detailed Vendor Profile B

Document access from the business perspective and verify it against technical evidence. A signed contract alone does not prove current access is appropriate.

VENDOR / THIRD PARTY

INTERNAL BUSINESS OWNER

CONTRACT START / END

NEXT ACCESS REVIEW

RISK RATING / RATIONALE

BUSINESS PURPOSE AND SERVICES PROVIDED

PEOPLE, ACCOUNTS, ROLES, AND PRIVILEGED ACCESS

SYSTEMS, APPLICATIONS, NETWORKS, LOCATIONS, AND PHYSICAL ACCESS

DATA ACCESSED, STORED, TRANSFERRED, OR CREATED

REMOTE-ACCESS METHOD, MFA, LOGGING, AND MONITORING

TOKENS, API KEYS, CERTIFICATES, INTEGRATIONS, AND SERVICE ACCOUNTS

SUBCONTRACTORS, DATA LOCATION, RETENTION, RETURN, AND DELETION

INCIDENT CONTACT, NOTIFICATION PERIOD, INSURANCE, AND CONTINUITY EVIDENCE

Quarterly Vendor Access Review

Verify current need, least privilege, machine identities, data handling, monitoring, dates, and evidence. Mark complete only after checking the relevant source.

- [ ] 1 The vendor still has a current business purpose, active contract, named internal owner, and approved access scope.
- [ ] 2 Every person uses an individual identity where possible; shared, generic, dormant, and former-worker accounts are removed or justified.
- [ ] 3 Access is limited to required systems, data, locations, hours, and functions; privileged access is exceptional and time-bound.
- [ ] 4 Multi-factor authentication is enforced for remote, cloud, administrative, and sensitive-data access.
- [ ] 5 Remote access uses an approved method and can be disabled centrally; unmanaged tools and persistent unattended access are reviewed.
- [ ] 6 Vendor access, administrative actions, file activity, and security alerts are logged and reviewed at a level appropriate to risk.
- [ ] 7 Data collection, storage, transfer, subcontracting, retention, return, and deletion match contract and business requirements.
- [ ] 8 The vendor's security, incident-notification, continuity, insurance, and subcontractor obligations remain adequate and evidenced.
- [ ] 9 Application tokens, API keys, integrations, certificates, service accounts, and automation credentials have owners and rotation dates.
- [ ] 10 Physical access, badges, keys, equipment, and facility permissions are current and limited.
- [ ] 11 Contract expiration, renewal, access-review, certificate, insurance, and termination dates are tracked with named owners.
- [ ] 12 Exceptions have written business justification, compensating controls, approving authority, owner, and expiration date.

VERIFIED BY	REVIEW DATE	NEXT REVIEW / CLOSE DATE

Vendor Access Termination Checklist

Coordinate business, legal, procurement, facilities, and IT actions. Removing the primary user account does not remove every path into the organization.

- [ ] 1 Confirm the termination date, exact access-disable time, internal owner, and whether legal or evidence-preservation requirements apply.
- [ ] 2 Disable vendor user accounts, privileged roles, remote access, VPN, portals, physical access, badges, keys, and registered devices.
- [ ] 3 Revoke active sessions, MFA methods, recovery methods, API keys, tokens, certificates, application passwords, and delegated access.
- [ ] 4 Rotate shared credentials, service-account secrets, door codes, emergency credentials, and any password the vendor knew.
- [ ] 5 Remove integrations, forwarding, automation, firewall rules, allowlists, trusted devices, and access from vendor-controlled networks.
- [ ] 6 Recover company equipment, documents, data copies, backups, credentials, and other assets; record anything missing.
- [ ] 7 Transfer system ownership, documentation, source files, configurations, domains, licenses, and support relationships.
- [ ] 8 Obtain required confirmation of data return or deletion, including subcontractors and backups where contractually applicable.
- [ ] 9 Retain necessary contracts, approvals, activity logs, communications, evidence, and deletion attestations.
- [ ] 10 Verify access removal independently across the system inventory; do not rely only on the vendor's confirmation.

VERIFIED BY	REVIEW DATE	NEXT REVIEW / CLOSE DATE

Exceptions, Remediation, and Approval

Do not normalize exceptions by leaving them open indefinitely. Each accepted risk needs an owner, compensating control, approving authority, and expiration date.

FINDING / EXCEPTION	RISK / IMPACT	REQUIRED ACTION	OWNER	DUE / EXPIRES

OVERALL RISK DECISION AND BUSINESS JUSTIFICATION

REVIEW OWNER

BUSINESS APPROVER

APPROVAL DATE