

Supplier and SaaS review worksheet

Clarify administrative ownership, data handling, continuity, notices and an orderly exit before purchase or renewal.

Purpose

Ask the same practical questions for each important provider. Record verified answers, documents and unanswered questions before committing to a service, renewing it or transferring ownership.

Prepare before the discussion

- The provider, service purpose, organizational owner and renewal date.
- A category-level description of records and important service dependencies.
- Available agreements, support terms and provider security information.

Review prompts - first half

1. Assign organizational ownership

Identify the business owner, technical administrator, contract contact and person authorized to renew or cancel. Avoid subscriptions that depend on a former volunteer's personal account.

2. Describe the information involved

Record data categories, permitted purpose, integrations and subcontractor questions. Use no real personal records in the worksheet.

3. Confirm account controls

Ask about MFA, individual administration, role permissions, access logs and recovery. Identify what the organization must configure and maintain.

4. Check access lifecycle

Confirm how staff, volunteer and provider access is approved, reviewed and removed. Include delegated and integration access.

5. Clarify continuity and backups

Distinguish provider availability from recoverability of the organization's data. Ask about restore scope, retention, export, recovery access and any separately required backup service.

Review prompts - continued

6. Understand support and notices

Record support hours, escalation routes and contractual incident-notice responsibilities. Confirm the organization's contact and after-hours decision owner.

7. Review evidence with context

Record the date and scope of provider assurance documents. Identify exclusions and unanswered questions; a logo or report title alone does not prove the organization's configuration is sound.

8. Plan data retention and disposal

Clarify deletion, backup retention, legal preservation and confirmation at contract end. Ask who can authorize and verify the outcome.

9. Rehearse the exit

Confirm usable export formats, transfer ownership, administrative account removal and dependency cleanup. Plan an authorized synthetic export check where available.

10. Make a documented decision

Record verified answers, material unknowns and the owner of follow-up work. Agree purchase, renewal or remediation with explicit responsibility and a review date.

Useful outputs

- A supplier record with ownership, responsibilities, verified evidence and open questions.
- A continuity and exit outline matched to the service's operational importance.
- A documented purchase or renewal decision and the next review date.

Review prompt

Use before purchase or renewal and after changes in ownership, data use, integrations or material service terms.

Your next decisions

Use this worksheet in your approved protected workspace. Record categories and decisions, not personal records, passwords, card data or recovery codes.

Scope / systems / programs: _____

Review owner: _____ Review date: _____

Topic / gap	Evidence / unknown	Owner / next action	Due / completion check

Where Layer8 can help

Cybersecurity: Assess the authorized scope, prioritize improvements and verify agreed safeguards.

Scope and use

This preparation worksheet does not replace contract review or a provider audit. Agree evidence requests and any testing with authorized provider and organizational owners.

Original Layer8 preparation prompts. Linked reference organizations do not endorse this guide.

Primary references

CISA: reducing supplier risk for small and medium businesses

<https://www.cisa.gov/resources-tools/resources/reducing-ict-supply-chain-risk-small-and-medium-sized-businesses-fact-sheet>

NIST: CSF quick-start guides

<https://www.nist.gov/cyberframework/quick-start-guides>

Online edition: [Layer8 resource library](#) / [supplier-saas-review](#)