

Donor and payment data review

Map record categories, exports, permissions, retention and the division of responsibility with payment providers.

Purpose

Follow the information from collection to disposal. Begin with categories and system ownership, then identify unnecessary copies, unclear permissions and decisions to confirm with the payment provider.

Prepare before the discussion

- The giving, accounting, email and program systems that handle or receive records.
- A category-level data-flow sketch and current access roles.
- Retention decisions, provider contacts and the merchant's existing compliance documentation.

Review prompts - first half

1. Describe each record category

Separate contact details, giving history, payment tokens, tax records and sensitive program records. Record why each category is needed without including personal values.

2. Trace collection and sharing

Identify forms, processors, imports, integrations, mailing lists, spreadsheets and exports. Assign an owner at each transfer.

3. Confirm payment scope

Ask the processor or acquiring bank to confirm payment handling, the applicable merchant validation process and responsibility boundaries. Outsourcing a payment channel still requires understanding the merchant's duties.

4. Review access and exports

Identify who can view, edit, export and administer records. Check access approval, MFA and removal after staff or volunteer changes.

5. Reduce unnecessary copies

Look for duplicate exports, personal mailboxes and files kept after a task ends. Agree a protected working location and a disposal owner.

Review prompts - continued

6. Agree retention and disposal

Confirm retention with the responsible business owner, counsel and accountant as appropriate. Identify what happens to exports and backup copies.

7. Separate sensitive program records

Evaluate children's, guardian, assistance and pastoral records separately from routine fundraising. Limit access to the people who need it for an approved purpose.

8. Clarify provider commitments

Review incident notice, subcontractors, data location, deletion and export terms. Record missing answers for the provider owner to obtain.

9. Plan a safe verification

Use synthetic records to verify permissions and exports. Do not send card numbers, security codes, donor histories or children's records through public contact forms or this website.

10. Record the decisions

Agree the permitted data flow, role changes and disposal actions. Assign owners and verify one representative completed change.

Useful outputs

- A category-level record and transfer map with named owners.
- Confirmed provider and merchant responsibilities, with unresolved questions recorded.
- Approved access, copy-reduction and retention actions with a completion check.

Review prompt

Revisit when adding a payment channel, integrating a new platform or changing record use and retention.

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 worksheet is preparation for a scoped review, not a PCI validation or a legal determination. Confirm payment obligations with the processor or acquiring bank and qualified advisers.

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

Primary references

PCI Security Standards Council: small-merchant resources

<https://www.pcisecuritystandards.org/merchants/>

NIST: small-business CSF quick-start guide

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf>

Online edition: [Layer8 resource library](#) / [donor-payment-review](#)