

Church and nonprofit audit preparation

Prepare a repeatable review of access, sensitive records, children's programs, continuity and accountable evidence.

Purpose

Turn a broad concern about security into a bounded first assessment. Use a U.S. operating baseline and a California applicability discussion where relevant; agree which systems, locations and workflows the review will cover.

Prepare before the discussion

- A list of systems, locations, providers and program owners, without customer or participant records.
- An outline of record categories, important workflows and current policies.
- The decision leadership needs, available participants and a safe review window.

Review prompts - first half

1. Agree the boundary

Identify locations, tenants, networks, payment channels and programs in scope. Record what is outside the review and who can authorize changes.

2. Map the sensitive records

List donor, member, child, guardian, support-service and workforce record categories. Identify purpose, storage, exports, access and retention. Use redacted or synthetic examples.

3. Review identity and volunteer access

Identify administrative roles, MFA and approved recovery routes. Trace one synthetic join, role change and departure through all important systems.

4. Walk through children's handoffs

Document check-in, pickup authorization and exception ownership. Rehearse an authorized pickup, a disputed pickup and an outage using synthetic records away from a live program.

5. Check the working environment

Account for office devices, kiosks, donated equipment, personal devices, guest Wi-Fi and AV systems. Compare intended boundaries with an agreed verification plan.

Review prompts - continued

6. Clarify payment responsibility

Identify payment providers and merchant responsibilities with the processor or acquiring bank. Record permitted handling and access; keep card numbers and security codes out of the assessment packet.

7. Review continuity and response

Identify critical services, protected contact routes, recovery priorities and decision authority. Plan a safe recovery exercise and a short incident discussion.

8. Resolve supplier ownership

Identify who owns each subscription, support relationship and administrative account. Clarify data exports, backups, incident notices and the exit process.

9. Confirm U.S. and California applicability

Ask qualified counsel which privacy, breach-notification, sector, grant and contract obligations apply. The California Attorney General states that CCPA generally does not apply to nonprofits; other duties need separate review. Record the applicability decision and its owner.

10. Agree evidence and the next decision

Separate observed controls, unknowns and gaps. Choose a small set of actions with an owner, a due date and a representative completion check. Review the result with leadership.

Useful outputs

- A bounded assessment scope, system and record-category inventory, and named evidence owners.
- A prioritized gap register with observation, impact, owner and next verification step.
- A leadership decision on remediation, responsibilities and the next review date.

Review prompt

Refresh before an assessment and after new programs, systems, locations or significant provider changes.

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 guide does not certify compliance or replace legal advice. Technical review of check-in systems complements the organization's safeguarding policy and trained staff.

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

Primary references

NIST: small-business CSF quick-start guide

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

California Attorney General: CCPA applicability FAQs

<https://oag.ca.gov/privacy/ccpa>

California Attorney General: breach reporting

<https://oag.ca.gov/privacy/databreach/reporting>

Online edition: [Layer8 resource library](#) / [church-audit-preparation](#)