Minimum Viable Evidence (MVE) for Security Questionnaires

Security questionnaires can eat days of your life—especially when every prospect asks for different screenshots, exports, and policies.

Minimum Viable Evidence (MVE) is a way to build a small, reusable "evidence pack" that answers 80–90% of what buyers and auditors ask for, without turning your team into full-time screenshotters.

This guide walks through:

- What MVE is (and isn't)
- The 8–10 evidence items most SaaS/AI/healthtech teams should have ready
- How to organize them so questionnaires stop being a fire drill

What Is Minimum Viable Evidence?

MVE is:

- The smallest set of proof that credibly demonstrates your security and privacy program
- Reusable across security questionnaires, audits, and investor due diligence
- Grounded in how you actually operate, not a fictional ideal

It is not:

- Every log, ticket, and config you've ever touched
- A replacement for real controls
- A one-time project you never update again

Think of it as your "go bag" for security reviews.

The Core MVE Set

For most 15–150 person SaaS, AI, and healthtech teams, a practical MVE pack includes:

1. High-level Security & Privacy Overview (2–4 pages or 10–12 slides)
    - What you do, who you serve, high-level architecture

- Key frameworks (SOC 2, ISO 27001/27701, HIPAA, GDPR/CCPA)
- Summary of your security and privacy program

2. Policy Pack (clean, current versions)
   - Information Security Policy
   - Access Control / IAM Policy
   - Incident Response Policy
   - Vendor/Third-Party Risk Policy
   - (Optional) Privacy / Data Protection Policy
3. Access Control Evidence
   - Screenshot or export showing SSO/MFA in use
   - Example of a recent privileged access review
4. Change Management / SDLC Evidence
   - Screenshot of your code review process (e.g., PRs)
   - Example ticket or record showing a change going through your process
5. Incident Response Evidence
   - Incident Response Plan (short, readable)
   - Record of a tabletop exercise or incident review in the last 12–18 months
6. Vendor & Subprocessor Evidence
   - Current vendor/subprocessor list
   - Example of a vendor risk review or security questionnaire you've completed on a key vendor
7. Data Protection & Privacy Evidence
   - Link or PDF of your current privacy notice
   - Example of how you'd handle a data subject request (internal playbook or checklist)
8. Training Evidence
   - Outline of your security/privacy onboarding
   - Record showing last training completion (e.g., screenshot from your LMS or attendance list)
9. Backups & Business Continuity Evidence
   - Brief description of backup strategy (what, how often, where)
   - Evidence of a recent restore test
10. Risk & Governance Evidence (optional but powerful)
    - Simple risk register or summary
    - Notes from a recent security/privacy review with leadership

You don't need these to be perfect—you just need them to be real, current, and easy to find.

How to Organize Your MVE Pack

- Create a single folder in your drive:
- `Internal > Evidence > Minimum Viable Evidence (MVE)`
- Inside, create subfolders by theme (Policies, Access, Change, Vendors, etc.).
- For each questionnaire or audit, pull from this folder first before creating anything new.

Set a quarterly reminder to:

- Remove obviously stale screenshots/exports
- Drop in any new evidence you've created for audits or big customers
- Update the Security & Privacy Overview if your architecture or scope has changed

Using MVE with Security Questionnaires

When a new questionnaire comes in:

1. Skim for themes (access, encryption, vendors, privacy, etc.).
2. Answer from your program first, not the form—use your MVE pack as the backbone.
3. Where a question goes beyond your current controls, be honest and explain your roadmap.

Over time, you'll find that:

- 70–80% of questions can be answered with copy-paste from your MVE pack
- The remaining 20–30% highlight genuine gaps or edge cases worth discussing

If you're constantly inventing new answers from scratch, your MVE pack isn't finished yet.