TRANSCRYPT

The Evidence Vault Blueprint: What to Collect and Why It Matters

Transform certification from stressful reconstruction to procedural submission. Learn exactly what evidence to collect for each of the five control areas, how to structure your vault, what auditors are really looking for, and how to maintain an evidence rhythm that eliminates panic.

If asked to prove a control tomorrow, do it in under two minutes.

Executive Summary

Most Cyber Essentials friction is not caused by weak security. It is caused by weak evidence.

Organisations often implement the right controls but fail to demonstrate them clearly. When assessment begins, they scramble through shared drives, email attachments, and half-forgotten screenshots trying to reconstruct proof after the fact. This is avoidable.

> An effective evidence vault transforms certification from a stressful reconstruction exercise into a procedural submission. The goal is simple: **If asked to prove a control tomorrow, you can do so in under two minutes.**

This guide explains exactly what to collect, how to structure it, what auditors are really looking for, and how to maintain an evidence rhythm that prevents last-minute panic.

You are not becoming an auditor. You are learning to anticipate one.

First Principle: Evidence Must Remove Doubt

Auditors are not searching for perfection. They are searching for confidence.

Good evidence answers three questions immediately:

- Does the control exist?
- Is it enforced?
- Is it current?

Anything that leaves interpretation introduces delay. The fastest certifications occur when evidence is unambiguous.

What an Evidence Vault Actually Is

Strip away the grand language. An evidence vault is simply a **central, structured repository** containing proof that your baseline security controls are operating.

It should be:

- Centralised
- Access-controlled
- Clearly labelled
- Easy to navigate
- Regularly updated

What it must never be is scattered. Fragmented evidence signals fragmented control.

Design the Vault Before You Fill It

Create structure aligned directly to the five Cyber Essentials control areas:

```
Evidence Vault
■
■■■ Firewalls & Internet Gateways
■■■ Secure Configuration
■■■ User Access Control
■■■ Malware Protection
■■■ Security Update Management
```

Inside each folder, separate by evidence type: Screenshots, Policies, Reports, Configuration exports.

Predictability is your ally. When auditors ask for something, you should know instinctively where it lives.

Control Area 1: Firewalls & Internet Gateways

What Auditors Want to See

They are confirming that uncontrolled inbound traffic is not permitted. Collect:

- Firewall configuration screenshots
- Rule summaries
- Confirmation that default passwords are changed
- Remote admin restrictions
- VPN configuration overview (if applicable)

If using a managed firewall, obtain a configuration summary from your provider. Ownership still rests with you.

Strong Evidence

Screenshot showing deny-by-default inbound rules, named device with visible timestamp, admin interface clearly identifiable.

Why it works: It demonstrates intent and enforcement simultaneously.

Weak Evidence

- A marketing datasheet for the firewall
- An invoice

- A vague statement such as "router configured securely"

Auditors assess controls, not purchases. Buying security tools is not the same as using them correctly.

Common Gap

Consumer routers in business environments. If present, ensure admin credentials are unique, firmware is current, and remote administration is disabled. Document this explicitly. Assumptions fail audits.

Control Area 2: Secure Configuration

This is about reducing attack surface. Auditors want proof that devices are hardened beyond factory defaults.

Collect:

- Device encryption status
- Screen lock enforcement
- Disabled unnecessary services
- Standard build documentation
- Mobile device controls (if applicable)

A single baseline build document is disproportionately valuable. It shows deliberate configuration rather than improvisation.

Strong Evidence

- Screenshot confirming full-disk encryption enabled
- Endpoint management console showing policy enforcement
- Build checklist used during deployment

These demonstrate repeatability. Repeatability signals maturity.

Inadequate Evidence

- A verbal assurance that "all laptops are encrypted"
- One screenshot from one device

Auditors extrapolate risk from sampling. Do not force them to guess.

Common Gap

Legacy machines quietly escaping the baseline. Perform a device inventory twice yearly at minimum. Unknown devices undermine otherwise solid posture.

Control Area 3: User Access Control

Identity is now the primary attack vector. Auditors examine it closely.

Collect:

- MFA enforcement screenshots
- Admin account list
- Joiner–mover–leaver process
- Password policy
- Privilege allocation approach

Clarity matters more than length. A one-page access philosophy often outperforms a ten-page policy nobody follows.

Strong Evidence

- Admin console showing MFA required for all users
- Screenshot listing privileged accounts
- Document describing least-privilege approach

This combination demonstrates governance.

Weak Evidence

- Policy without proof of enforcement

- MFA enabled for "most" users

"Most" is not a defensible security position. Consistency is the standard.

Common Gap

Dormant accounts belonging to former staff. Run quarterly access reviews. Remove hesitation from this process. Disable first, investigate second if necessary.

Control Area 4: Malware Protection

Auditors are not testing brand preference. They want assurance that malicious code is unlikely to execute undetected.

Collect:

- Endpoint protection dashboard screenshot
- Real-time protection status
- Signature update confirmation
- Device coverage report

Central visibility is critical. If protection is installed but unmanaged, risk remains opaque.

Strong Evidence

- Console view showing all devices protected
- Alerts panel visible
- Update status current

This communicates operational awareness.

Weak Evidence

- Screenshot from a single laptop
- Proof of purchase

Again, ownership of the control matters more than acquisition.

Common Gap

Bring-your-own-device environments without defined protection expectations. If personal devices access company data, your policy must state required safeguards. Ambiguity invites audit friction.

Control Area 5: Security Update Management

Attackers disproportionately exploit known vulnerabilities. Patch discipline is therefore heavily scrutinised.

Collect:

- Patch management dashboard
- Update policy
- Exception handling process
- Evidence of supported operating systems

A written patch cadence is surprisingly persuasive. It signals operational rhythm.

Strong Evidence

- Screenshot showing devices fully updated
- Automated patch policy
- OS version visibility

These eliminate interpretive burden.

Weak Evidence

- Statement that "updates are automatic"
- One device shown as current

Auditors care about estate-wide posture.

Common Gap

Unsupported operating systems lingering in corners. These frequently derail certification. Retire them or isolate them decisively. There is no elegant workaround.

Good vs. Inadequate Evidence — The Underlying Pattern

Strong evidence is:

- Current
- Estate-wide
- Clearly labelled
- Hard to misinterpret

Weak evidence is:

- Partial
- Old
- Device-specific
- Ambiguous

When in doubt, ask: **Would a cautious stranger feel confident relying on this?** If not, improve it.

The Evidence Labelling Standard Most Businesses Skip

Adopt a simple naming convention:

```
[ControlArea]_[System]_[WhatItShows]_[YYYY-MM-DD]
```

Example:

```
AccessControl_M365_MFAEnforced_2026-02-08
```

This prevents forensic file hunting later. Small operational habits produce large renewal advantages.

The Monthly Collection Calendar

Evidence gathering should be ambient, not frantic.

Monthly (15–20 minutes)

- Capture patch dashboard
- Confirm endpoint protection coverage
- Export MFA status
- Note any new infrastructure

Minimal effort. Maximum future relief.

Quarterly (45–60 minutes)

- Review admin accounts
- Validate firewall posture
- Confirm encryption coverage
- Update device inventory

Think of this as posture verification rather than compliance work.

Annually

- Refresh policies

- Archive superseded evidence
- Remove obsolete devices from records
- Validate that your vault structure still fits your environment

Do not allow the repository to decay into clutter. Order supports confidence.

Evidence Mistakes That Cause Certification Delays

Over-Collection. Hundreds of files with no hierarchy create noise. Auditors prefer precision.

Under-Collection. Sparse evidence invites questions. Questions slow certification.

Outdated Screenshots. Timestamp visibility matters more than many realise.

Personal Storage. Evidence on individual machines introduces fragility. Centralise always.

Teach Your Organisation to Generate Evidence Passively

The strongest environments produce proof as a byproduct of operation. For example:

- Endpoint dashboards naturally show coverage
- Access platforms log MFA
- Patch tools generate reports

When selecting tools, consider their evidentiary clarity. Visibility is not administrative vanity. It is operational leverage.

Think Like an Auditor (Without Becoming One)

Adopt three mental checks:

Visibility. Could an outsider understand this quickly?

Consistency. Does evidence align across devices?

Recency. Is it obviously current?

If all three are satisfied, certification friction drops sharply.

When Evidence Signals Deeper Problems

Occasionally, difficulty producing proof reveals genuine control weakness. Treat this as valuable intelligence rather than inconvenience.

Evidence gaps often expose:

- Informal device deployment
- Privilege sprawl
- Patch inconsistency
- Tool fragmentation

Correction strengthens both security and audit readiness.

The Strategic Value Most SMEs Miss

An organised evidence vault does more than support certification. It:

- Accelerates procurement responses
- Reassures insurers
- Strengthens client trust
- Enables faster incident investigation
- Supports operational continuity

In short, it professionalises your security posture.

Build Once. Benefit Repeatedly.

The first vault requires intention. After that, maintenance is trivial compared to reconstruction.

Future renewals should feel administrative precisely because your environment is observable.

Security that cannot be demonstrated is security that will be doubted.

Final Guidance

Do not treat evidence as paperwork created for auditors. Treat it as a reflection of operational control.

Build a vault that is:

- Structured
- Current
- Unambiguous
- Centralised

Then maintain it quietly throughout the year.

When certification arrives, you should not prepare. You should simply submit.

Ready to Build Your Evidence Vault?

Visit **transcrypt.xyz** for templates and tools to help you structure your evidence vault and maintain audit readiness.