

Compliance is being run on spreadsheets

Not because anyone chose to — because nothing else held all of it at once.

The workbook starts as a convenience and becomes the system of record. Then a second framework arrives, and a second workbook. Then evidence lives in a shared drive, findings live in an email thread, and the only person who knows how it fits together is the analyst maintaining it. **The assessment was never the hard part.** Keeping it consistent, current and provable is.

Inconsistency

THE SAME CONTROL, THREE ANSWERS

Multi-factor authentication is asked about by Cyber Essentials, ISO 27001, the CAF and NIS2. In four workbooks it gets four answers, written months apart, by different people, against no shared evidence. Nobody can say which one is true.

Time

SPREADSHEET MANAGEMENT, NOT RISK

Copying answers between tabs. Re-chasing evidence already collected for another framework. Rebuilding the board slide by hand every quarter. It is skilled people doing clerical work, and it scales linearly with every framework added.

Decay

TRUE ON THE DAY, STALE BY THE QUARTER

A workbook records what was true when it was filled in. It does not know the certificate lapsed, the supplier changed hands, the OS went out of support, or that the reassessment and the risk review were due six weeks ago.

THE COST, ITEMISED

THE JOB	ON SPREADSHEETS	WHAT IT ACTUALLY COSTS
Answering a control	Once per framework	The same question is researched and evidenced four or five times, and the answers drift apart.
Knowing where you stand	Manual roll-up	A position that is out of date the moment it is built, and cannot be reproduced later.
Turning gaps into work	A second tracker	Findings and actions live apart, so nothing links a closed task back to the gap that caused it.
Running the ISMS	A workbook per register	Risks, assets, the RACI and the Statement of Applicability in separate files, scored against a method nobody approved and reviewed when someone remembers.
Proving it to an assessor	Folder archaeology	Days reconstructing which evidence supported which answer, on which date.
Reporting upward	A slide rebuilt each quarter	Hours of collation for a single number that is already out of date when it is presented.
Staying current	A calendar reminder	Nothing watches the frameworks, the suppliers or the estate between assessments.

THE SAME PROBLEM AT THREE SIZES

Under 50 people

One person is the compliance function, part-time, alongside another job. Cyber Essentials is the immediate need; a customer will ask for ISO 27001, and the ISMS behind it, within the year. There is no capacity to run two programmes in parallel — so the second one gets started late and rushed.

50 – 1,000 people

Two or three analysts, four or five frameworks, a supplier list nobody owns end to end, and a board that wants one number. Most of the week goes on collation rather than judgement.

1,000+ / group

Separate scopes per business unit or system, overlapping regulatory regimes, and evidence held by teams who do not report to compliance. Consistency across scopes is the whole difficulty.

THE THREE FIXES THAT DON'T HOLD

A BIGGER SPREADSHEET

Adds tabs, not consistency. The cross-framework duplication is still there, still manual, and now harder to audit.

AN ENTERPRISE GRC SUITE

Priced and scoped for a team that already exists. Months of configuration before it answers its first question, and the content is yours to author.

AN ANNUAL CONSULTANT

Produces a good report and leaves. The findings still land in a spreadsheet, and nothing watches the eleven months in between.

Security Compliance Hub is not an assessment tool with extra screens. There are two ways in: an assessment, or your ISMS. What it is for is the operating loop that follows: one evidence base across every framework, findings that become owned work, risks that are managed rather than remembered, and a position that stays current between assessments.

Answer it once

Every other framework that asks the same thing already knows what you said.

Twenty frameworks, more than 2,400 questions, and a great many of them are the same control asked in different words. When a framework is finalised, its answers become available to every other framework that has a genuine relationship to them — shown against the question being answered, with the source, the wording and the date.

Is there a maintained, up-to-date inventory of all hardware assets supporting essential functions?

Cross-framework references below are Security Compliance Hub's own analysis relating similar requirements across frameworks — not an official or certified equivalence.

CLOSELY RELATED Cyber Essentials: "Do you maintain a software inventory or asset register?": We have one but it's not regularly updated (finalised 2026-08-14).

PARTIALLY RELATED Cyber Essentials: "Do you have a process to track when software will become unsupported?": Yes, we track support end dates and plan accordingly (finalised 2026-08-14).

CLOSELY RELATED ISO 27001 A.5.9-5.10: "Is there an inventory of information and associated assets, with defined acceptable use rules?": Partially Implemented (finalised 2026-09-02).

All servers, network devices, endpoints, OT/ICS equipment, and other hardware supporting essential functions should be inventoried with owner, location, criticality, and support lifecycle status.

Achieved

Partially Achieved

Not Achieved

Not Applicable

One CAF outcome, three references. Two from a finalised Cyber Essentials run, one from ISO 27001 — each with the question that was asked, the answer given and the date it was confirmed. Illustrative data.

IT SUGGESTS. IT NEVER ANSWERS FOR YOU.

A reference is context, not a pre-filled box. Nothing is ever auto-selected on your behalf, and every block carries a standing note that the relationship is Security Compliance Hub's own analysis rather than a certified equivalence. An assessor can see exactly what informed an answer.

20 frameworks

2,400+ questions

17 authored crosswalk tables

34 directions

THE SAME EVIDENCE, EVERYWHERE IT IS NEEDED

EVIDENCE VAULT

- ▶ A file is attached **to the question**, not to a folder — so the same policy PDF answers the ISO clause, the CAF outcome and the CE control at once.
- ▶ Import straight from **SharePoint**, so the document stays where it is governed.
- ▶ Connected tools — **Entra ID, Okta, CrowdStrike, Google Workspace** — supply live signal against the questions they genuinely bear on.

CONSISTENT ACROSS SCOPES, AND ACROSS PEOPLE

NAMED SCOPES

A group can run the same framework several times over — one per business unit, system or essential function — each tracked, finalised and archived on its own, each contributing its own cross-framework references. No second account, no duplicated workbook, and the default run is untouched.

WHERE THE RELATIONSHIPS COME FROM

Hub	CE · CAF · ISO 27001 · CIS NIST CSF · NIS2 · DCC
Official	CMMC ↔ FedRAMP (NIST SP 800-171 mapping)
Official	HIPAA ↔ NIST CSF 2.0 (NIST SP 800-66 Rev 2)

PROOF, NOT RECOLLECTION

- ▶ **Assessment Archive** keeps the question-by-question record of every finalised run — wording, answer, evidence note, files — for three years.
- ▶ **Audit Pack** exports the whole thing as a ZIP with SHA-256 integrity hashes, the risk management documents included, for a certification body to review offline.
- ▶ **Compliance Passport** prints the one-page board summary that used to be rebuilt by hand each quarter.

ONE DRAFT, SEVERAL PEOPLE

Progress syncs across devices and across the team, with the last editor named and a section lock so two people do not overwrite each other. The answer stops living on one analyst's laptop, which is where most of the inconsistency starts.

What this removes. The second, third and fourth research pass on a control you have already evidenced — and the argument, six months later, about which workbook was right.

A score is not an outcome

What happens to the findings is the part that changes anything.

On spreadsheets, a finished assessment produces a number and a list. The list is copied into a tracker, the tracker drifts, and next year's assessment starts again from nothing. Here the findings stay attached to the assessment that produced them, and carry an owner, an effort estimate and a state.

Opportunistic Ransomware via Phishing

5 of 7 frameworks

NCSC CAF
DORA
Cyber Resilience Maturity
NIST CSF 2.0

CRITICAL

+ Add to Risk Register

NIS2 Directive Compliance Assessment

Business Email Compromise (Invoice Fraud)

5 of 7 frameworks

NCSC CAF
DORA
Cyber Resilience Maturity
NIST CSF 2.0

HIGH

+ Add to Risk Register

NIS2 Directive Compliance Assessment

Credential Stuffing → Account Takeover

5 of 7 frameworks

NCSC CAF
DORA
Cyber Resilience Maturity
NIST CSF 2.0

HIGH

+ Add to Risk Register

NIS2 Directive Compliance Assessment

Lost or Stolen Device → Data Exposure

5 of 7 frameworks

NCSC CAF
ISO 27001
Cyber Resilience Maturity
NIST CSF 2.0

HIGH

+ Add to Risk Register

NIS2 Directive Compliance Assessment

Signals, not per-framework noise. The same weakness seen by five different frameworks is one finding, ranked by how many corroborate it — not five separate rows to reconcile. Illustrative data.

33%

complete

2 critical

1 high

1 medium

4 open of 6

NCSC CAF	1 critical	2 open / 2 total	Continue →
Cyber Essentials	1 critical	1 open / 2 total	Continue →
ISO 27001	0 open / 1 total		Continue →
Cyber Resilience Maturity	1 open / 1 total		Continue →

One worklist across every framework. Actions are created from the analysis, keyed to the run that produced them, and counted together rather than per workbook. Illustrative data.

WHAT AN ANALYST STOPS DOING

- ▶ Re-typing findings into a separate tracker, then keeping the two in step.
- ▶ Working out by hand whether two frameworks are complaining about the same thing.
- ▶ Chasing owners by memory, with no record of what was agreed.

WHAT THE PLATFORM DOES INSTEAD

- ▶ Creates the actions from the analysis, **idempotently** — re-running does not duplicate them.
- ▶ Corroborates a finding across frameworks before ranking it.
- ▶ Carries owner, urgency and effort on the action, and shares it with the team.

THE LOOP, ONCE ROUND

1 · Assess

Answer the framework, with references from what you have already finalised elsewhere.

2 · Corroborate

Weaknesses seen by more than one framework are ranked above those seen by one.

3 · Act

Actions carry an owner, an urgency and an effort estimate, and are shared with the team.

4 · Retain

What outlives the fix becomes a register entry with a disposition and a named owner.

Findings expire. Risks do not. A finding is a point-in-time observation; some of what it reveals is a standing risk the organisation lives with, accepts or transfers. Those belong somewhere that outlives the assessment — which is the next page.

Point-in-time is how you get caught out

Your ISMS, the trend, and everything that watches in between.

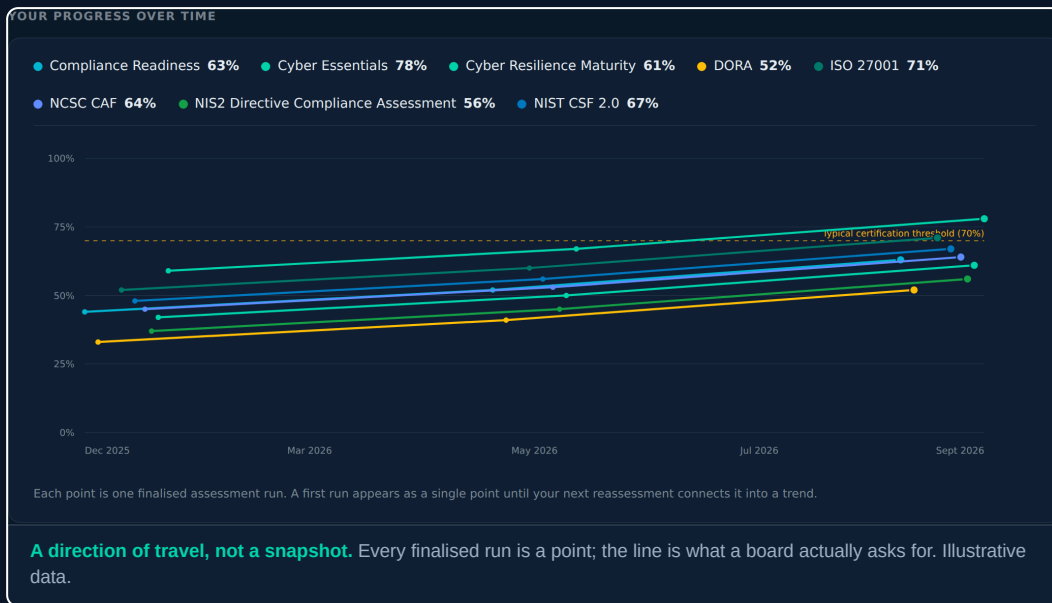
RISK MANAGEMENT

ISO 27001, ISO 42001 or the CAF on one page: assets, method, RACI, register, Statement of Applicability, AI impact assessments and reviews. Nothing waits for an assessment; rules, not AI, decide.

- ▶ Risks are added by hand or from a risk signal or remediation action, and keep their source.
- ▶ Each is scored inherent and residual against the method you approved, owned through the RACI, treated, and accepted where it fits.
- ▶ Assessment questions show notes from these records; the Audit Pack carries the documents.

Risks					
RISK	OWNER	INHERENT	RESIDUAL	TREATMENT	NEXT REVIEW
Ransomware encrypts depot systems the depot warehouse system and file shares Organisation-wide	ISMS lead Sam Okafor	20 Critical	8 Moderate	Treat - 3 of 4 actions done	8 Nov 2026
Phishing leads to a finance account takeover the finance SaaS platform ISO 27001: Head office ISMS	Finance director Priya Shah	16 High	6 Moderate	Treat - complete - accepted 20 Oct 2026	29 Mar 2027
Backup restore never tested end to end the warehouse system and finance data Organisation-wide	Infrastructure lead Tom Ellis	15 High	10 Moderate	Treat - 0 of 1 action done	12 Nov 2026

The register: owners, residual risk and reviews. Illustrative data.



WHAT WATCHES BETWEEN ASSESSMENTS

Reassessment	30 / 7 / 0 days, then overdue	A digest and an in-app banner before a framework's annual mark passes, not after.
Risk reviews	On your method's schedule	Each risk falls due at its band's interval; overdue and due within 30 days are listed.
Frameworks	16 sources, weekly	The published standards themselves are monitored for change, with a content diff on what moved.
Your estate	Weekly vendor lifecycle sync	Declared software is checked against real vendor end-of-life dates, never a guess.
Suppliers	Weekly re-scan	Third-party posture is re-checked and drift raised as an alert — see the Third Party Risk sheet.
Peers	Sector benchmark	Your score against anonymised peers in your sector, once ten have contributed.

WHAT IT TAKES TO START

Nothing to install

Browser only. No agent, no appliance, no migration. Connectors are optional and read-only.

Start with one framework

Finalise it, and the next one begins with its questions already informed.

Or with your ISMS

The register, method, RACI and assets don't need an assessment. Assess when it has taken shape.

Or run a portfolio

For MSPs and vCISOs: per-client tenancy, scoped team access, portfolio risk ranking and each client's ISMS.