

Answer once. See everywhere it counts.

The Hub links the questions of your frameworks, so work done for one shows in the others.

Most frameworks ask about the same controls in their own words: MFA, backups, incident response, supplier checks. The Hub's crosswalks link those questions one by one. Once you finalise an assessment, its answers show under the related questions of your other frameworks, and **Across your frameworks** lists the gaps they share, ranked by how many frameworks one fix counts in. Rules do the linking and the ranking: no AI is used, and a link never changes an answer.

12

frameworks in the hub

25

tables, each read both ways

1,172

links between questions

619

of them close, the rest partial

Which frameworks are linked, and how closely



CLOSE OR PARTIAL

- ▶ **Close:** the two questions ask for the same thing, so the evidence for one usually serves the other.
- ▶ **Partial:** they overlap, but one asks for more or less. The link's note says how.
- ▶ **Direct links only.** A shared gap never joins two questions through a third framework, since partial links would chain together questions that aren't alike.

THE TWO PAIRS NIST MAPS

CMMC ↔ FedRAMP

200 links, from NIST's mapping of SP 800-171 to SP 800-53.

HIPAA ↔ NIST CSF 2.0

461 links, from NIST SP 800-66 Rev 2, carried to CSF 2.0 by NIST's own transition mapping.

On these two pairs the note goes further and **suggests an answer**, translated from yours. It's still only a suggestion.

What you answered elsewhere, under the question you're answering

Once one framework is finalised, its answers show under the related questions of the others.

Is multi-factor or continuous authentication enforced for internal staff accessing critical systems?

CLOSELY RELATED Cyber Essentials: "Is Multi-Factor Authentication (MFA) enabled on ALL cloud services?": Yes, MFA is enabled on all cloud services (finalised 2026-10-20).

CLOSELY RELATED NCSC CAF B2.a — Identity Verification, Authentication and Authorisation: "Is multi-factor authentication (MFA) enforced for all users accessing systems supporting essential functions, especially for remote and privileged access?": Partially Achieved; "Are authentication mechanisms appropriate to the sensitivity of the systems accessed, and are authorisation decisions based on least privilege?": Not Achieved (finalised 2026-10-13).

CLOSELY RELATED ISO 27001 A.8.2-8.5: "Are privileged access rights restricted and managed, with information access restrictions and secure authentication mechanisms enforced?": Partially Implemented (finalised 2026-10-06).

CLOSELY RELATED NIST CSF 2.0: "Is multi-factor authentication enforced for all staff accessing critical systems, remote access and administrative interfaces?": Implemented (finalised 2026-10-10).

CLOSELY RELATED DORA Article 9(4)(c) and (d): "Is there a robust identity and access management policy including strong authentication, least-privilege access, and regular access reviews?": Achieved (finalised 2026-09-29).

NIS2 Article 21(2)(j). Stolen credentials remain the single most common way attackers gain initial access — NIS2 calls out MFA by name rather than leaving it buried inside general access control.

► What good looks like

On the NIS2 assessment. The MFA question shows what was answered on the related questions of five other finalised assessments, each with how closely it's linked and the date it was finalised. Illustrative data.

HOW IT WORKS

- **Finalised answers only**, never a draft, so what shows is what was signed off. Each named scope's run shows too, labelled with its name.
- **Each framework in its own note**, never merged into one judgement.
- **Your answer stays yours**. A note never fills it in, and a line above the first one says the links are our own analysis, not an official equivalence.
- **For MSPs and vCISOs**, each client's notes come from that client's own assessments.

WHERE ONE ASKS FOR MORE, THE NOTE SAYS SO

DORA, UNDER ITS LINK TO NIS2'S EARLY WARNING

"DORA's initial notification is due within 4 hours of classifying the incident as major, and no later than 24 hours after becoming aware of it..."

SOC 2 READINESS, UNDER ITS OPERATING QUESTIONS

"A SOC 2 Type II audit samples evidence from across its period, usually 3 to 12 months..."

UK GDPR, UNDER ITS LINK TO ISO 27001'S INCIDENT HANDLING

"ISO 27001 sets no deadline: a notifiable personal data breach goes to the ICO without undue delay and, where feasible, within 72 hours..."

HOW A LINK IS MADE

By hand, question by question

Each link is written from both frameworks' own text and graded close or partial, with a note naming the clause, Article or criterion it rests on.

One table, read both ways

A table is written in one direction and read back in the other, so a link shows on both frameworks' pages.

No counterpart, no link

CAF's threat hunting has no ISO 27001 question to link to, and UK GDPR's lawful basis none either, so neither is linked. A link to a question that doesn't exist fails our tests.

THE ASSESSMENTS THAT SHOW THEM

Cyber Essentials

NCSC CAF

ISO 27001

CIS Controls v8.1

NIST CSF 2.0

NIS2

DORA

DCC Readiness

SOC 2 Readiness

UK GDPR

ISO/IEC 42001

AI Governance

CMMC Level 2

FedRAMP Moderate

HIPAA Security Rule

The last three, in blue, are linked through NIST's mappings: CMMC with FedRAMP, and HIPAA with NIST CSF 2.0.

Fix once, and it counts in several

Where one fix counts in several frameworks, and where work done in one is waiting to count in another.

Open it with **Shared gaps** on My Hub. It compares your finalised assessments question by question through the crosswalks and works out, by rules, where one piece of work would count in several of them.

1
Is information security maintained during disruption, and is ICT continuity planned and tested against your recovery objectives?
Counts in 5 frameworks

Starts from ISO 27001 A.5.29-5.30 · 4 close links

▼ The 7 linked questions

FRAMEWORK	QUESTION	ANSWER	LINK
ISO 27001 A.5.29-5.30	Is information security maintained during disruption, and is ICT continuity planned and tested against your recovery objectives? ● Partially Implemented	● Partly	Starts here Open
NCSC CAF B5.a	Resilience Preparation Has the organisation identified and documented single points of failure for systems supporting essential functions? ● Achieved Are recovery time objectives (RTO) and recovery point objectives (RPO) defined for essential functions and reflected in system design? ■ Not Achieved	■ Not in place	Close Open
NIS2 BCM_3	Are your business continuity plans tested on a defined, regular basis? ■ Not Achieved	■ Not in place	Close Open
NIS2 BCM_1	Have you conducted a business impact analysis for your critical systems and services? ■ Not Achieved	■ Not in place	Partial Open
NIS2 BCM_5	Do you have a crisis management plan for cybersecurity incidents, with a defined crisis team and communication procedures? ● Partially Achieved	● Partly	Partial Open
DORA Article 11	Is there a comprehensive ICT business continuity policy with documented response and recovery plans? ■ Not Achieved	■ Not in place	Close Open
NIST CSF 2.0 PR_15	Have recovery time and recovery point objectives been defined, tested and validated for all critical systems? ■ Not Implemented	■ Not in place	Close Open

Add to tracker

One shared gap, five frameworks. ISO 27001's continuity question, linked to CAF, NIS2, DORA and NIST CSF 2.0, and fully in place in none of them. Each row shows the answer given and how closely it's linked. Illustrative data.

- ▶ **Ranked by how many frameworks one fix counts in**, then how many have it not in place, then how closely they're linked.
- ▶ **Add to tracker** files one Remediation Tracker item under the framework you choose, naming the questions it also closes. A later analysis never removes it.
- ▶ **Already in place in** another framework: that work may be the starting point.
- ▶ **Compare a named scope**, such as one essential function's CAF beside the ISO 27001 scope covering the same systems.
- ▶ **Print it for the board**, or export CSV or JSON.

For MSPs and vCISOs: each client's Across frameworks tile in the MSP Portal opens the same page for that client and says how many shared gaps it has.

IN PLACE · CYBER ESSENTIALS

Does every user have their own unique account (no shared logins)?

Yes, every person has their own unique account, finalised 20 Oct 2026

NOT YET · NIST CSF 2.0 PR_1

Do you manage user identities with unique named accounts and enforce least-privilege access principles?

Partially Implemented, finalised 10 Oct 2026

[Open the NIST CSF 2.0 question →](#)

Done in one, not yet in another. In place in Cyber Essentials, partly in NIST CSF 2.0: the evidence may already exist. Illustrative data.

Across your frameworks needs two linked frameworks finalised. The Assessment Bundle (Solo and Team), Risk Operations and the MSP plans include every framework in the crosswalk hub. The crosswalks are Security Compliance Hub's own analysis of which questions address a similar concern, not an official or certified equivalence; the CMMC ↔ FedRAMP and HIPAA ↔ NIST CSF 2.0 pairs follow NIST's published mappings. A link never changes an answer. Screens are the shipped product showing a fictional organisation; answers and dates are illustrative.