

NIST Cybersecurity Framework

A plain guide to the NIST Cybersecurity Framework and CSF 2.0: the six functions, how tiers and profiles work and how it lines up with NIS2 and ISO 27001.

WHAT IT IS

The NIST Cybersecurity Framework is a voluntary set of cybersecurity outcomes from the US National Institute of Standards and Technology. It gives any organisation a common language to assess, prioritise and communicate cyber risk. It is a reference, not a product or a certification, and CSF 2.0 now applies to organisations of any size or sector.

WHY IT MATTERS

6 functions

Govern, Identify, Protect, Detect, Respond and Recover in CSF 2.0

NIST CSF 2.0, 2024

16.6bn dollars

reported US cybercrime losses in 2024, up 33% on the year

FBI IC3, 2024

30%

of US organisations already used the framework by 2015

NIST, citing Gartner, 2016

WHAT HAPPENED

In 2024 the ALPHV/BlackCat group reached Change Healthcare through a remote-access portal that had no multi-factor authentication. The missing MFA was confirmed in congressional testimony, a 22 million dollar ransom was paid and the data was still exposed. The breach reached 192.7 million people, the largest healthcare data breach in US history. MFA on remote access is a Protect outcome (PR.AA).

RED FLAGS TO WATCH FOR

Signs your controls are not yet framed

- No single owner is accountable for cybersecurity at board level
- Remote access, VPNs or portals that a password alone can reach
- No list of which suppliers hold or process your data
- Backups that have never been tested by an actual restore
- Security spending that follows the newest tool, not a ranked gap

THE ONE RULE THAT STOPS IT

Compare where you are with where you need to be, then fix the biggest gap first. Build a Current Profile across the six functions, set a Target Profile and let the gap set your priorities.

THEN BUILD THE HABIT AROUND IT

- Name an accountable owner and write the core policies (Govern)

- Turn on MFA for every remote-access path (Protect)
- Keep a current supplier register and manage their risk (Govern, GV.SC)
- Test your backups and your recovery plan on a schedule (Recover)
- Reassess the profiles yearly and after any major change

MYTHS AND FACTS

MYTH

You can be certified in NIST CSF.

FACT

There is no official NIST CSF certification. It is a voluntary reference, though its functions map to certifiable standards such as ISO 27001.

MYTH

The CSF and the NIST Risk Management Framework are the same.

FACT

They differ. The CSF is a voluntary outcome model, while the RMF (SP 800-37) is a mandatory seven-step process for US federal systems.

MYTH

Adopting the framework means you have met NIS2 or DORA.

FACT

It helps, but it is not the same. The framework organises your controls and evidence, yet each regulation keeps its own legal thresholds and deadlines.

THE LEGAL DUTY

In Sweden, NIS2 and Cybersäkerhetslagen (SFS 2025:1506, in force 15 January 2026) require risk management, incident handling and supply-chain security under Article 21, and make the board accountable under Article 20. Each duty maps onto a CSF function, which is why the framework is useful evidence.

GET HELP

Talk to eBuilder Security about mapping your controls to the NIST CSF and aligning them with NIS2 and Cybersäkerhetslagen.

[Read the Full Article →](#)