PENTESTERRA

NIST CSF 2.0 GAP ASSESSMENT

Are Your 6 Cybersecurity Functions Actually Covered?

Gap assessment across all 106 subcategories of the NIST Cybersecurity Framework 2.0, spanning the 6 functions Govern, Identify, Protect, Detect, Respond, Recover.

IN SHORT

Covers all 106 subcategories of NIST CSF 2.0 across the 6 functions (GV Govern, ID Identify, PR Protect, DE Detect, RS Respond, RC Recover) and 22 categories. Technical subcategories are auto-filled from your scan evidence.

106
NIST CSF 2.0 subcategories covered

6
Functions: Govern, Identify, Protect, Detect, Respond, Recover

Voluntary
A reference framework increasingly demanded by clients and insurers

THE SITUATION TODAY

WHO YOU ARE

You're the CISO of an organization using (or looking to adopt) the NIST CSF as its reference framework for cybersecurity posture - voluntary, but increasingly requested as a baseline.

WHAT HAPPENED

A board, a cyber insurer, or an enterprise client asks for a mapping of your posture against the NIST CSF - not just a list of tools you've installed.

WHY IT HURTS

Without a real mapping, 'we follow the NIST CSF' stays a claim, not proof - and an insurer or client notices the difference.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.

THE SOLUTION

Pentesterra's NIST CSF 2.0 Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.

WHY IT'S DIFFERENT

You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of NIST CSF 2.0, grouped the way you'll see them in the platform.

Govern and Identify

The two functions that establish strategy and risk visibility.

- Cybersecurity risk management strategy
- Asset, data and supplier inventory
- Roles, responsibilities and policies

Protect

The safeguards to limit or contain a cybersecurity event.

- Identity management and access control
- Awareness and training
- Data and platform security

Detect

The activities to discover anomalous events in a timely manner.

- Continuous security monitoring
- Adverse event analysis

Respond and Recover

What to do during and after an incident.

- Incident management and communication
- Recovery planning and execution

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for NIST CSF 2.0

A complete report, ready to present to clients, auditors, or your board.

Request your NIST CSF 2.0 Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance