CYBER360
TRUSTED SECURITY ADVISOR

SERVICE BROCHURE

CYBER360 / SPECIALIST SERVICES

NIST Cybersecurity Framework

Clear scope. Practical evidence. Lasting improvement.

Translate cybersecurity frameworks into a practical security programme. Cyber360 helps you select relevant frameworks, assess current outcomes and build an implementation roadmap aligned with your risks and business priorities.

01 Clear scope

02 Practical evidence

03 Priorities for improvement

TRUSTED SECURITY ADVISORY

Advice that leads to action.

cyber360.co | info@cyber360.co | Standards & assurance

01 / SCOPE & FOCUS

The right question. A useful assessment.

Translate cybersecurity frameworks into a practical security programme. Cyber360 helps you select relevant frameworks, assess current outcomes and build an implementation roadmap aligned with your risks and business priorities.

Framework selection & scope

Business services, risks, obligations, stakeholder expectations and existing standards.

A selection rationale and defined assessment scope.

Current & Target Profiles

Selected NIST CSF 2.0 outcomes across Govern, Identify, Protect, Detect, Respond and Recover.

Current and Target Profiles with a prioritised gap view.

Unified control mapping

Existing controls and mappings to selected frameworks and obligations.

A control catalogue, mapping and responsibility matrix.

Governance, policies & risk

Roles, oversight, policy architecture, risk methodology and supplier expectations.

Tailored policies and a practical risk-management process.

Implementation & enablement

Agreed technical, administrative and physical control work packages.

Implementation guidance, awareness materials and an action roadmap.

Measurement & maintenance

Metrics, evidence repositories, review cycles and programme reporting.

A reporting model, evidence checklist and maintenance calendar.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Set the objective

Agree scope, frameworks, stakeholders and business priorities.

Establish the baseline

Review current controls and evidence against selected outcomes.

Define the target

Agree desired outcomes and priorities with accountable owners.

Plan and implement

Sequence agreed improvements and supporting documentation.

Measure progress

Review evidence and report outcomes, gaps and remaining risk.

Maintain the programme

Reassess after change and update profiles, mappings and actions.

WHAT YOU RECEIVE

Leadership & programme owners

- Framework selection and scope rationale.
- Current and Target Profiles or equivalent gap baseline.
- Prioritised roadmap with owners and dependencies.
- Governance metrics and review priorities.

Control & delivery teams

- Mapped control catalogue and responsibilities.
- Policy and risk-assessment documentation.
- Implementation guidance and evidence requirements.
- Awareness materials and maintenance procedures.

03 / PREPARATION & NEXT STEPS

Start with the right context.

Scope & objectives

• Identify services, systems and the assurance question driving the work.
• Share relevant obligations, stakeholder expectations and target dates.

Evidence & context

• Provide existing policies, risk assessments, architecture and prior findings.
• Identify suppliers and dependencies relevant to the agreed scope.

People & ownership

• Nominate business, technical, risk and operational contacts.
• Confirm decision authority and ownership of implementation actions.

Delivery & follow-up

• Agree work packages, access, constraints and acceptance criteria.
• Scope independent assurance, system changes and active testing explicitly.

PRACTICAL QUESTIONS

Is NIST CSF a certification?

No. NIST CSF is a framework of cybersecurity outcomes. This work supports its use; it does not provide a NIST-issued certification or regulatory approval.

Does CSF 2.0 have six functions?

Yes: Govern, Identify, Protect, Detect, Respond and Recover. These functions organise outcomes across cybersecurity risk management.

Consulting applies to the agreed scope. Independent assurance, certification or attestation and active testing are separately agreed. No successful outcome is guaranteed.

Reference: NIST Cybersecurity Framework (October 2026).

LET’S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

Contact Cyber360 to discuss your requirements.