CYBER360
TRUSTED SECURITY ADVISOR

CYBER360 / SPECIALIST SERVICES

Cyber Resiliency

Clear scope. Practical evidence. Lasting improvement.

Connect continuity planning, incident response and recovery around the services your business depends on. Cyber360 helps you identify dependencies, agree recovery priorities and exercise the plans before an incident puts them under pressure.

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.

Connect continuity planning, incident response and recovery around the services your business depends on. Cyber360 helps you identify dependencies, agree recovery priorities and exercise the plans before an incident puts them under pressure.

Business continuity planning

Critical services, people, suppliers, facilities and business-impact assumptions.

A continuity plan and prioritised dependency map.

Disaster recovery

Selected applications, infrastructure, identity services and recovery dependencies.

A recovery strategy, runbook actions and validation plan.

Incident response readiness

Incident roles, escalation, containment authority and response playbooks.

Response playbooks and a tabletop exercise plan.

Ransomware recovery readiness

Backup arrangements, isolation, privileged access and selected recovery environments.

A readiness assessment and prioritised recovery improvements.

Crisis communications

Leadership, staff, customers, partners, regulators and media contacts where applicable.

A communications plan and scenario-specific message templates.

Resilience exercises & learning

Tabletops, restoration tests and failover drills selected for the agreed objective.

An exercise report, lessons and accountable improvement actions.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Define critical services

Agree business objectives, dependencies and disruption scenarios.

Assess the readiness

Review continuity, response, backup and recovery evidence.

Set recovery priorities

Agree objectives, sequencing, owners and operational constraints.

Develop usable plans

Build or update agreed runbooks, playbooks and communications.

Exercise safely

Run the agreed scenario with monitoring, permissions and stop conditions.

Improve and repeat

Track actions and schedule revalidation as the environment changes.

WHAT YOU RECEIVE

Leadership & business owners

- Business-impact and dependency findings.
- Continuity priorities and recovery objectives.
- Crisis decision and communications responsibilities.
- A phased resilience improvement roadmap.

Response & recovery teams

- Agreed continuity, response and recovery playbooks.
- Backup and restoration readiness findings.
- Exercise plan, observations and lessons.
- Action register with owners and revalidation criteria.

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 this the same as disaster recovery?

No. Disaster recovery focuses on restoring technology. Cyber resiliency also addresses critical business services, people, suppliers, response decisions and adaptation.

Will you test production failover?

Only where explicitly scoped and approved. We agree safeguards, dependencies, monitoring, rollback and stop conditions before any disruptive test.

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

Reference: NIST cyber resiliency guidance (October 2026).

LET’S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

Contact Cyber360 to discuss your requirements.