

CYBERSECURITY

ETHICAL HACKING

PENETRATION TESTING

TRAINING



NIS2 Compliance

Gap analysis, remediation plan and training to achieve and maintain compliance



OBJECTIVE

Turn obligations and deadlines into a **resilience programme**

The NIS2 Directive requires demonstrable governance, risk management, technical measures and response capabilities.

ISGroup translates requirements into operational priorities aligned with the organisation, sector and exposure.

METHOD

From gap analysis to an **actionable, verifiable plan**

Assessment

We map scope, obligations, governance and existing measures.

Remediation plan

We order actions by risk, dependencies, cost and deadlines.

Implementation

We support controls, procedures, training and evidence collection.

DELIVERY

Governance, supply chain, incidents and **business continuity**

The programme covers risk management, supplier security, vulnerabilities, access, backup and incident response.

Management roles and responsibilities are formalised through escalation and reporting flows.

Training and exercises make controls effective in day-to-day operations.



Soddisfare i requisiti di Compliance



KEY STRENGTHS

GRC and technical expertise in the same delivery team

Coverage

Organisational, documentary and technical requirements assessed together.

Priorities

Actions ordered by real risk and delivery capacity.

Evidence

Decisions, controls and checks documented for audits and authorities.



OUTPUT

A NIS2 roadmap with ownership, deadlines and **evidence**

Gap analysis against applicable requirements.

Prioritised remediation plan with owners and deadlines.

Evidence register for controls, training and verification.

Management reporting for progress and residual risk.

Let's **HACK** together



ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

BOOK A MEETING
sales@isgroup.it
+39 045 4853232