RADIUM
TECHNOLOGIES

Compliance Shield

A Managed Cybersecurity Compliance & Resilience Service

- Supporting DORA, NIS2, GDPR, ISO 27001 & more
- Radium Cybersecurity & Compliance Services
- Delivering continuous compliance, resilience & audit readiness

RADIUM
TECHNOLOGIES

Market Problem
& Drivers

Why Compliance Shield is Needed

- Rapidly evolving regulatory landscape (DORA, NIS2, CBI ICT, GDPR, PCI DSS)
- Increasing regulatory scrutiny and audit expectations
- Lack of integrated cyber resilience + compliance frameworks
- Fragmented tooling, policies, and reporting
- Limited incident response readiness across organisations

Organisations struggle to move from compliance on paper →operational resilience in practice

RADIUM
TECHNOLOGIES

Compliance Shield

Overview

A structured suite of services delivering:

- Regulatory alignment
- Risk management
- Governance & policy support
- Continuous compliance & audit readiness

Built on proven frameworks:

- NIST CSF 2.0
- ISO/IEC 27001 / 27005 / 22301
- NIST SP 800-30 / 61
- COBIT / ITIL

RADIUM
TECHNOLOGIES

Regulatory
Alignment

Aligning to Key Regulations

- DORA – Digital Operational Resilience
- NIS2 – Network & Information Security Directive
- GDPR – Data protection & breach reporting
- ISO 27001 – Information Security Management
- PCI-DSS / Cybersecurity Act / CBI ICT Guidelines

Ensures organisations are audit-ready and regulator-aligned

Capabilities:

- Control mapping & gap analysis
- Regulatory interpretation
- Evidence & audit trail creation
- Compliance dashboards
- PCI-DSS / Cybersecurity Act / CBI ICT Guidelines

RADIUM
TECHNOLOGIES

Risk Management
Framework

Integrated Cyber Risk Management

- Ensures organisations are audit-ready and regulator-aligned
- Threat, vulnerability & impact analysis
- Business Impact Assessment (BIA)
- Risk register & remediation tracking
- Alignment with ISO 27005 & NIST RMF

Outputs:

- Risk heatmaps
- Prioritised remediation plans
- Continuous risk monitoring

Moves organisations from reactive → risk-driven decisionmaking

RADIUM
TECHNOLOGIES

Security Monitoring & Incident Response

Operational Cyber Resilience

- Centralised Security Monitoring (SIEM/SOC integration)
- Threat detection & alerting
- Incident Handling & Response (IH&R) framework
- Crisis Management Team (CMT) integration
- DR Test Events & cyber simulations

Enables rapid detection, response, and recovery

Based on:

- NIST SP 800-61
- ISO 27035
- SANS IR methodology

Governance

& Policy Support

Establishes clear accountability and control

Building a Strong Governance Framework

- Information Security Governance model
- Policy, standards & procedures development
- Role definition (CISO, Risk, IT Ops, Audit)
- Reporting structures & executive dashboards
- Third-party & supply chain risk governance

Deliverables:

- Policy templates
- Governance frameworks
- Compliance reporting packs

RADIUM
TECHNOLOGIES

Security Awareness & Training

Embedding a Culture of Compliance

- Staff awareness programmes (DORA/NIS2 obligations)
- Role-based training (IT, Risk, Execs)
- Incident response simulations & tabletop exercises
- Playbooks for governance, risk & IR teams

Additional:

- Knowledge base
- Stakeholder engagement frameworks

Transforms compliance into organisation-wide responsibility

RADIUM
TECHNOLOGIES

Continuous Compliance
& Audit Readiness

Sustaining Compliance Over Time

- Continuous compliance monitoring
- Metrics & KPIs (NIST SP 800-55 aligned)
- Regular audits & reassessments
- Regulatory update tracking
- DR Test Events & recovery validation

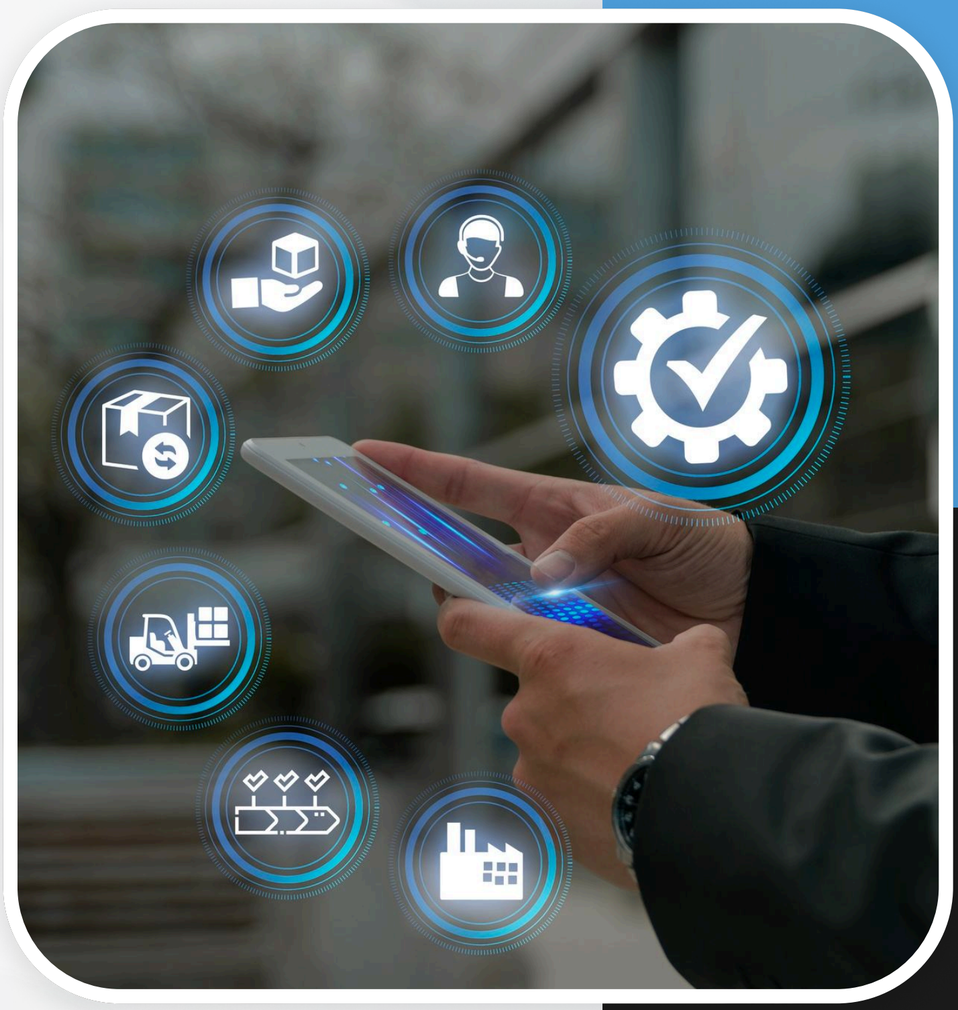
Ensures ongoing compliance, not one-time certification

Outputs:

- Compliance dashboards
- Audit reports
- Improvement roadmaps

RADIUM
TECHNOLOGIES

Delivery Model
& Value Proposition



How Compliance Shield is Delivered

- Advisory
- Implementation
- Managed Service (Compliance-as-a-Service)

Core Components:

- Governance framework setup
- Risk & compliance tooling
- Incident response capability
- Audit readiness & reporting

Business Value:

- Reduced regulatory risk
- Faster audit cycles
- Improved cyber resilience
- Measurable compliance maturity