Securing Connectivity

Deliver continuous telecoms resilience and supplier assurance for Telecoms Security Act (TSA) compliance

Assured telecoms resilience

The UK Telecoms Security Act (TSA) places clear and enforceable obligations on communications providers to protect the security and resilience of critical telecoms infrastructure.

Meeting these obligations requires more than implementing technical controls; organisations must demonstrate strong governance, continuous assurance, and a clear understanding of risk across networks, IT applications and infrastructure, assets, and supply chains.

CGI can help telecoms providers operationalise TSA requirements through structured resilience assessments and supplier assurance capabilities that align regulatory expectations with real-world operations.

The challenge

Regulatory expectations are no longer theoretical; TSA compliance is now actively enforced. Ofcom has set clear expectations around proactive supervision, targeted information requests, and demonstrable ongoing assurance.

Organisations that are unable to show how risks are identified, prioritised, and managed in practice face increased scrutiny, remediation activity, and potential enforcement action.

For Chief Information Security Officers (CISOs) and security leaders, the challenge is not control implementation alone. Point-in-time assessments, static documentation, and fragmented assurance models no longer meet regulatory expectations. TSA requires evidence that security and resilience risks are understood, governed, prioritised, and continuously managed across networks, services, assets, and suppliers.

Across the sector, we see common issues, including:

1. Translating outcome-based TSA and the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) requirements into consistent, repeatable operational assessments.
2. Maintaining visibility of critical assets, service tiering and dependencies across complex and virtualised environments.
3. Providing consistent board-level reporting and evidence of risk-based decision-making.
4. Managing assurance across multi-vendor supply chains and managed service providers (MSPs).
5. Bridging the gap between policy compliance and real operational resilience.

Organisations primarily regulated by the TSA include Public Electronic Communications Network (PECN) providers, and Public Electronic Communications Service (PECS) providers. In practice, this includes mobile and fixed network operators, internet service providers (ISPs), and wholesale and infrastructure providers.

TSA obligations are risk-based, rather than size-based. Smaller operators with national reach or strategic interconnectivity may face obligations comparable to tier-one mobile network operators (MNOs)

The scope often extends beyond the traditional network perimeter. Cloud-hosted telecom platforms, network function virtualisation providers, and managed service providers are frequently drawn into scope through contractual and assurance requirements.

As networks become more virtualised and supplier ecosystems more complex, assurance and governance models do not always evolve at the same pace. This creates material risk.

When responding to TSA obligations, telecoms organisations commonly struggle with:

1. Converting outcome-based CAF objectives into practical, repeatable assessments.
2. Maintaining accurate asset inventories and service tiering across complex estates.
3. Demonstrating effective board oversight, accountable risk ownership and ongoing risk management.
4. Operating continuous assurance across multi-vendor supplier ecosystems.
5. Producing clear, defensible evidence for regulatory scrutiny.

The solution

TSA resilience assessments with automation

CGI helps telecoms organisations move from point-in-time compliance to continuous resilience status reporting.

We work with you to understand your operational context, services and systems to help transform and operationalise your resilience. By combining expert-led TSA resilience assessments with automation, we provide ongoing insight into your security and operational posture. This approach replaces static reporting with continuous visibility across critical networks, systems, and suppliers.

Our TSA resilience assessment solutions enable you to:

- Assess and evidence resilience against TSA obligations and the NCSC CAF.
- Monitor security and resilience continuously, rather than relying on periodic reviews.
- Detect misconfigurations and vulnerabilities automatically across critical environments.
- Generate real-time resilience scores to identify emerging risks early.
- Prioritise issues based on service criticality, regulatory impact, and operational risk.

Our services and solutions support key TSA requirements across governance, risk management, asset management, service tiering, and supplier oversight. They adapt as frameworks, regulatory expectations, and threat landscapes change.

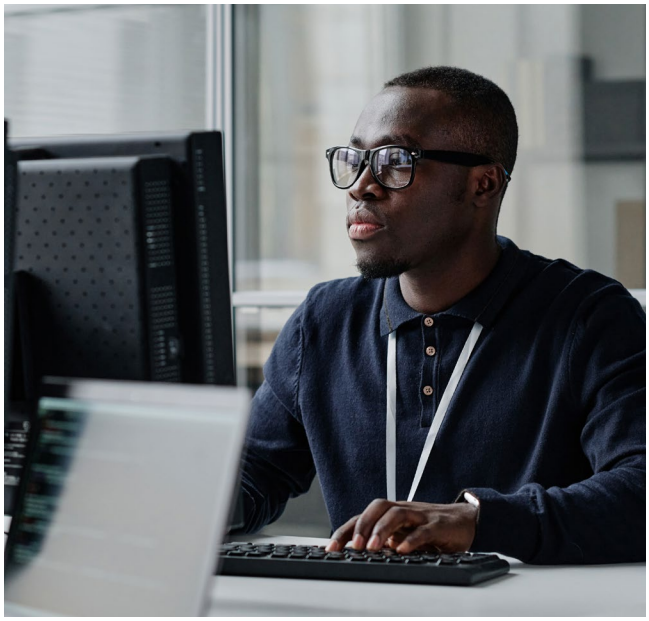
The benefits for your organisation

You gain a clear, regulator-ready view of your TSA posture, backed by evidence you can trust.

By combining automation with deep regulatory expertise, we help you:

- Reduce manual effort through automated assessments and monitoring.
- Improve resilience across networks, platforms, and third-party suppliers.
- Focus teams on the risks that matter most to critical services.
- Demonstrate continuous compliance with confidence, not assumptions.
- Support informed investment decisions using real operational insight.

CISOs and security leaders are able to clearly demonstrate how risks are prioritised, how resilience is measured across critical services, and how investment decisions are informed by real operational insights. This builds confidence with regulators, partners, and internal stakeholders.



Supplier assurance

Securing your supplier ecosystem

Suppliers are integral to your operational environment and, crucially, part of your attack surface. CGI's supplier assurance services enable transparent, proportionate and auditable supplier security oversight.

Our solutions help you establish ongoing, risk-based oversight of third parties that support critical telecoms services. We combine expert assurance with automation to give you continuous visibility, not periodic checks.

Our approach enables you to:

1. Assess supplier controls against recognised standards and TSA expectations.
2. Automate supplier evidence collection and assurance workflows.
3. Apply risk-based supplier tiering and prioritisation.
4. Identify high-risk suppliers early, before they affect service resilience.
5. Maintain a transparent and auditable supply-chain security model.

Why act now?

The TSA places clear responsibility and accountability on telecoms providers to manage risks across suppliers and the wider telecoms ecosystem.

Our supplier assurance services help you evidence active supplier risk governance through:

1. Proportionate, ongoing supplier oversight aligned to TSA obligations.
2. Defensible reporting suitable for regulators, boards, and audit.
3. Reduced operational exposure by turning supplier assurance into a managed control.

This gives you confidence that supplier risks are understood, prioritised, and addressed before they become service-impacting issues.

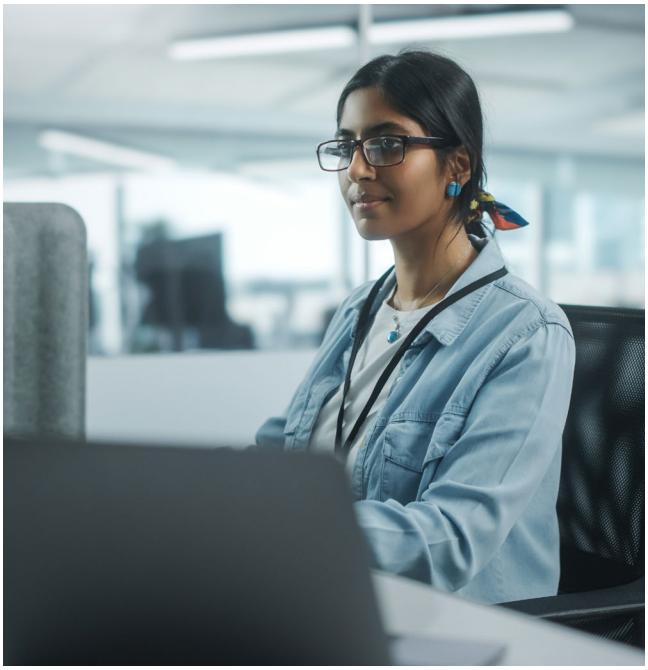
Key capabilities aligned to TSA

CGI combines deep cyber security expertise with decades of experience delivering and operating services for regulated telecoms and Critical National Infrastructure (CNI).

We understand how TSA requirements apply in real operational environments, not just on paper. This means our assurance models are practical, implementable, and designed to work at scale.

Our clients benefit from automation embedded directly into assurance, reducing manual effort while improving accuracy and timeliness. We bring proven experience working with boards, regulators, and accountable owners - helping organisations evidence control, oversight, and informed decision-making.

Our capabilities scale seamlessly from advisory through to implementation and managed services, supporting both immediate TSA compliance needs and long-term telecoms resilience.



Our key capabilities include:

- TSA readiness assessments and gap analysis.
- Governance framework design and implementation.
- Cyber risk management aligned to service criticality.
- Threat-led testing, including red and purple teaming.
- Third-party and supplier risk management.
- Business continuity management and disaster recovery planning.
- API-led integrations for continuous monitoring.
- Real-time risk and resilience dashboards.
- Cross-standard compliance mapping, including TSA and NCSC CAF.
- Ongoing assurance, reporting, and operational oversight.

What this means for your organisation

By using our TSA-aligned cyber resilience and supplier assurance services, you gain confidence, clarity, and control.

For CISOs and security leaders:

1. Clear visibility of security and resilience across critical services, assets, and suppliers.
2. Reduced regulatory risk through continuous, evidence-based assurance.
3. Actionable insights focused on material risk, not generic control lists.
4. Defensible reporting that stands up to regulatory and board scrutiny.

For the organisation:

1. Reduced risk of TSA enforcement action, fines, brand dilution, and reputational damage.
2. Improved operational resilience and service continuity.
3. Stronger supplier governance and reduced third-party risk exposure.
4. Lower cost and effort through automation and reduced manual activity.
5. A scalable assurance model that adapts to evolving TSA requirements, technology, and threats, and maps easily to other frameworks.

CGI helps you move beyond compliance to demonstrable, operational telecoms resilience. Your posture becomes trusted by regulators and clearly understood by the board.

Our focused TSA readiness and assurance review helps you understand your current exposure, priority gaps, and regulatory risk. This provides a clear, board-ready view of where you stand and what actions matter most.

To discuss how we can support your TSA obligations and wider telecoms resilience objectives, contact our Cyber Security consulting team.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-focused to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cgi.com/uk/cyber-security | Email us at cyber.enquiry.uk@cgi.com