Deloitte.

# Unravelling the Telecommunications Security Act

# Introduction

The **Telecommunications Security Act 2021** (TSA) is a new piece of legislation which amends the Communications Act 2003: It introduces new security requirements on providers of *public electronic telecommunications networks and services* ('Providers'). The TSA came into force on 1st October 2022 and contains compliance requirements across a number of security domains.

In this paper we will unpack the TSA, provide our insights and help clients to focus on key areas which could be time consuming to implement and embed. We will also introduce Deloitte's TSA Companion Tool (TCT) and its content pack that has been specifically created to measure and record compliance with the TSA.

What is the long-term significance of the TSA?

- **Non-compliance may result in fines:** The TSA gives Ofcom oversight and responsibility powers. Providers are able to provide a level of visibility and rationale in their cyber strategy which should be used when communicating with Ofcom.
- **Brand reputation:** Where a Provider fails to meet defined security measures or provide rationale, this could lead to reputational damage and negatively impact shareholders.
- **Investment required:** Clear levels of investment on both CapEx to uplift capabilities and OpEx to sustain cyber capabilities will be required.
- **Wider network implications:** Third parties, joint ventures and merged networks all fall within the scope of the TSA. It is important to have strong visibility over the entire network to have effective controls and assurance.

Code of Practice Terms:

**"Shall":** Indicates that there is likely to only be one viable technical solution to secure the network or service in line with the regulations.

**"Should":** The government views the solution provided as being the best way to implement the measures in the majority of cases.

**"May":** Indicates that Providers are likely to have multiple options, all of which could deliver a satisfactory solution.

**Non-compliance with the guidance measures:**

'..We appreciate that where the regulations require Providers to take 'appropriate and proportionate' measures, what is appropriate and proportionate will depend on the particular circumstances. Providers may comply with new security duties and specific security requirements by adopting different technical solutions or approaches to those specified in the code of practice.'

'...A public telecoms provider may choose to comply with those new security duties and specific security requirements by adopting different technical solutions or approaches to those specified in the code of practice.'

## The TSA – What you may have missed

1. *Code of Practice Terms:* Although the code of practice contains detailed measures across a number of security domains, Ofcom has included specific *terms* that should be considered and used in accordance with the measures defined. The three key terms *"Shall", "Should"* and *"May"* are defined on the left.

2. *'appropriate and proportionate'* – The guidance set out in this code of practice is not the only way for providers to comply with the new security duties and specific security requirements. Providers are empowered (in some instances) to determine what is '*appropriate and proportionate'* against their own circumstances.

## Deloitte are well positioned to help:

Deloitte's TSA Companion Tool (TCT) integrates seamlessly with TSA requirements. This can be leveraged to provide visibility across a Provider's network, as a solution for tracking compliance activities across phases and a medium to communicate rationale with Ofcom.

In the next pages of this paper, we will introduce the TSA *tiering system* which sets out the different expectations and timelines for large and medium-sized public telecommunications providers and explore our views of where effort should be focused.

# TSA Tiers and Layers

The Telecommunications Security Act (TSA) is part of a wider expansion of regulatory requirements now referred to as the 'Three Layer Framework'. The TSA also sets out the 'tiering system' which classifies telecommunication providers based on their size and UK annual revenue. TSA compliance requirements and timelines depend on where Providers are classified in this system.

## The TSA Tiering System

The TSA categorises Providers into different tiers (see table 1).

The term 'Phase' is the grouping terminology we have used to categorise all the technical and procedural guidance controls (measures) according to their compliance deadlines. Providers will need to adhere to the deadlines of each phase.

Tier 1 and 2 Providers must align with the Code of Practice requirements described in the Three Layer Framework below.

| TSA Tier System | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| **Size of Business** | Large | Medium | Small |
| **Annual Revenue Criteria** | > £1 Billion | £1 Billion - £50 Million | < £50 Million |
| **Phase 1** | 31 March 2024 | 31 March 2025 | N/A – No mandatory compliance requirements |
| **Phase 2** | 31 March 2025 | 31 March 2025 | |
| **Phase 3** | *31 March 2027 | 31 March 2027 | |
| **Phase 4** | 31 March 2028 | 31 March 2028 | |

**Code of Practice Compliance Deadlines**

*Table 1: The TSA Tiering system Please note there is a group of measures, Third Party Supplier Measures 3, with 54 controls and its own deadline – Tier 1: 31st March 2024 & Tier 2: 31st March 2025 for **new** third party contracts and for **all existing** third-party contracts by 31st March 2027.*

## The Three Layer Framework

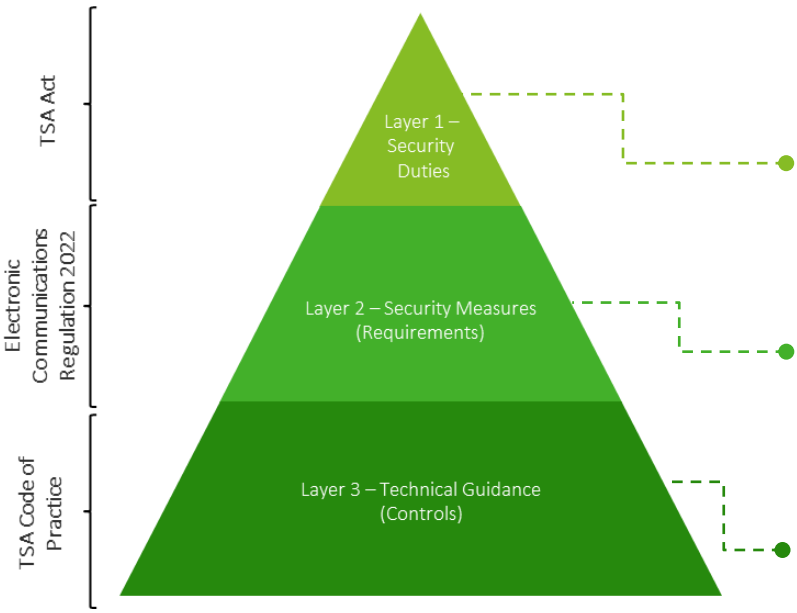



*Figure 1: The Three Layer Framework*

The Framework comprises of three discrete layers, creating a robust model to engage with emerging security risks and opportunities.

**Layer 1 – Strengthened Overarching Security Duties on Telecommunication Providers :** Layer 1 mandates service providers to maintain greater security, handle breaches effectively and inform Ofcom of any security compromises.

**Layer 2 – Specific Security Measures (Requirements):** Layer 2 details the security measures to be taken in addition to Layer 1, including compliance with the Electronic Communications (Security Measures) Regulations 2022.

**Layer 3 – Technical Guidance :** At the core of legislation, Layer 3 contains detailed technical guidelines and controls for Tier 1 and 2 Providers. This encourages a holistic approach to security and drives transformational changes, not just tick-box exercises to avoid fines.

The technical requirements outlined in Layer 3 will be central in defining a roadmap towards phased compliance. In the following page we will describe each Phase and based on what we know, anticipate higher complexity areas for Providers.

# Phases of the TSA

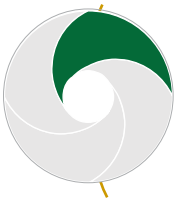
An understanding of the phases is vital for Providers aiming to fulfil their obligations under the Act. A focus on adaptability, forward planning and resilience is key to remain in control. Each phase has a range of measures with a variety of focus areas designed to help navigate providers on a path towards TSA compliance. We refer to each group of related measures as separate domains.

All Tier 1 and Tier 2 Providers are required to adhere to the same measures for each phase. It is important to start at the beginning as latter phases augment the fundamental security practices established in Phase 1.

For each phase we have detailed the relevant domain groupings for each phase of TSA compliance.

**Our Insights:**

Based on what we know, we have highlighted areas we believe have higher complexities for design, through to implementation and operate.



## PHASE 1 | 46 Measures

**Overarching | Management Plane 1 | Signalling Plane 1 | Third Party Supplier Measures 1 | Supporting Business Processes**

The key concepts are aligned to the NCSC Cyber Assessment Framework standards, including foundational concepts such as zero trust architecture and holistic privileged access management.

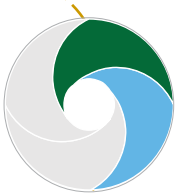
**Higher complexity areas** = Network architecture and defining strategic planning.

## PHASE 2 | 31 Measures

**Management Plane 2 | Signalling Plane 2 | Third Party Supplier Measures 2 | Customer Premises Equipment**

Phase 2 delves further towards defence in depth strategies. These reflect a layered approach to network and "exposed edge" security, addressing points of vulnerability.

**Higher complexity areas** = Network segmentation, data privacy and source validation.



## PHASE 3 | 105 Measures

**Management Plane 3 | Signalling Plane 3 | Third Party Supplier Measures 4 | Virtualisation 1 | Monitoring and Analysis 1 | Network Oversight Functions**

This phase introduces advanced and complex concepts such as virtualisation security, intrusion detection, log synchronisation and host-based sensing. These topics emphasise the need for multi-faceted defences to ensure a comprehensive view of security.

**Higher complexity areas** = Penetration testing and fuzzing, privileged access workstations and threat intelligence sharing.

## PHASE 4 | 22 Measures

**Management Plane 4 | Signalling Plane 4 | Virtualisation 2 | Monitoring and Analysis 2 | Retaining National Resilience Capability**

The final phase requires a solid understanding of data and privacy best practices, including obfuscating customer data and network topology information. Automation is key with an emphasis on automated prioritisation of tasks, including business continuity, event management and administration processes.

**Higher complexity areas** = Automation, business continuity planning, data obfuscation and sovereignty.

A comprehensive understanding of each phase of measures is key to adhering to the TSA. To further understand the responsibilities of each phase, we have broken down the key concepts in the next page with our SME insights.

# Key concepts for each phase

The phased journey to building and sustaining cyber resilience in line with the TSA is different for every Provider and is shaped by current state and priorities. We believe the following five concepts are the most important for Providers to consider when defining transformation activities aligned to the TSA.

Key: Type of transformation

- Large scale organisational change with communications
- Increase visibility of Provider network
- Uplift processes and rationale

| Key Concept | Insights |
|---|---|
| **Network Architecture**<br>Phases 1, 2, 3 and 4 | The TSA Code of Practice is founded on both the **NCSC Anti-Pattern** for network segmentation and the **Microsoft Enterprise Access Model** for Administrative segregation. This combination drives Providers towards **a zero-trust centric architecture** which will be challenging for Providers with legacy security controls and technology platforms. |
| **Identity and Access Management**<br>Phases 1, 2, 3 and 4 | This encourages a shift towards an Enterprise Access Model and **emphasises the use of Privileged Access Workstations (PAWs)** with stringent hardening requirements including OS hardening, zero-trust architecture, whitelisting applications and full encryption. Providers should ensure they have dedicated PAWs that only have access to the internet for security-critical functions via VPN and dedicated PAWs with access to internal-only business systems. |
| **Supply Chain & Third-Party Management**<br>Phases 1, 2 and 3 | Whilst not everything in the TSA is in direct control of the Provider, **is it essential that Providers have visibility** of which organisations are providing them with services. This could even lead to a fourth party organisation where controls and assurance will need to be applied to **mitigate supply chain risks**. The TSA defines an approach to assess a vendor's security processes and their supplier network equipment. |
| **Resilience**<br>Phases 1, 2, 3 and 4 | Providers consistently face recovery delays due to **a mismatch between what is recovered by technology and what is needed by the business.** Providers should continue to shift from solely relying on an incident playbook to **diversifying their recovery capabilities**. One such TSA requirement is to secure offline backups by keeping them digitally disconnected, regularly create new back-ups and ensure backups can restore live operations. |
| **Governance**<br>Phases 1, 2, 3 and 4 | Providers need **clear communication channels** for reporting risks and a **culture of transparency**. For example, where a Provider's Data Protection Officer (DPO) does not hold a senior role, the DPO should still have direct access to the Provider's board. Enabling regular risk assessment processes for operational changes, with security team involvement is essential for effective governance. |

Telecommunication providers have transformed rapidly over the last 10 – 20 years, reflecting advancements in network architecture and identity management. The TSA is a catalyst for providers to accelerate strategic change and for senior management and their boards to evaluate the business impact of operational disruption. On the next page we introduce Deloitte's TSA Companion Tool (TCT) which enables this by giving Providers a communication tool, visibility and rationale

# Deloitte's TSA Companion Tool

## The Deloitte TSA Companion Tool (TCT) is exactly what is needed to support TSA activities, both now and in the future.

Our **intuitive solution** measures compliance against the TSA and is a **visible instrument** by which Providers can **communicate progress** to stakeholders and regulators.

The TCT **directly supports Management Planes 1 – 4** using structured and proven methodologies to define current and target cyber maturity levels.

We have **integrated dashboards**, shown below, for reporting holistically across measures and the **overall cyber resilience** of Providers.

## We are strong security implementation partners.

Providers require support with the implementation of their TSA activities to ensure they meet objectives in the fastest, most efficient manner. Deloitte offers a customisable suite of cyber solutions and managed services to accelerate such activities.

### Advisory

We provide insights, expertise and strategies for Providers to become TSA compliant. By understanding your enterprise-wide needs, we can advise you and your teams on decisions across the business. The TSA requires Providers to be resilient and so security must be factored into strategic direction and investments.

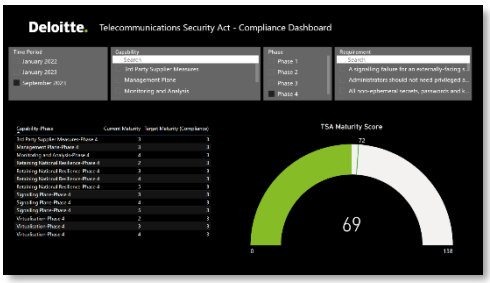
### Transformation

The TSA is a driver for threat-led security transformations. We support Providers to improve their underlying infrastructure and capabilities. This is needed to embed the right people, processes and technologies to deliver real value to the business.

### Operate

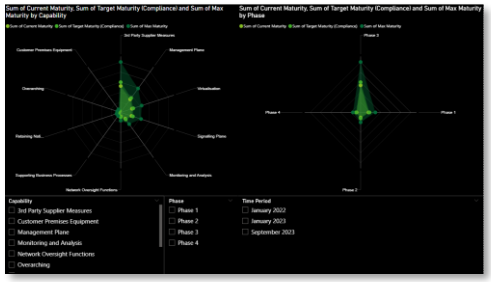
Our Operate services accelerate security management operations for Providers. We bring together the tools and skills needed to actively monitor and manage your threat landscape for the TSA. One such service is Digital Identity by Deloitte which leverages cloud-based technologies to evolve identity management capabilities.

## TCT Toolset and Integrated Dashboards



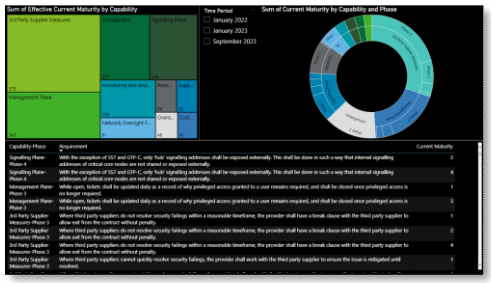

### Maturity dashboard

A central view showing the gap between your current and target maturity and relevant benchmarks.



### Radar chart

A dual-diagram visual that compares phases with capabilities in a visual way for senior leaders.



### Capability view

The sunburst view and heat map allows you to examine specific TSA requirements in terms of maturity and resilience.

The capability view is especially important because it will indicate areas of least maturity based on the inherent exposure scores and different threat scenarios. This supports the TSA domains of **Signalling Planes 1 - 4, Virtualisation 1 - 2** and **Network Oversight Functions.**

# How Deloitte can help

Drop us a note to get the conversation started and to discuss your journey in unravelling the Telecommunications Security Act.

**Susan Sharawi**
Partner
Technology & Transformation | Cyber
ssharawi@deloitte.co.uk

**Neal Aggarwal**
Partner
Technology & Transformation | Enterprise Technology & Performance
neaggarwal@deloitte.co.uk

**Saleen Chowdhury**
Senior Consultant
Technology & Transformation | Cyber
saleenchowdhury@deloitte.co.uk

Deloitte.