semperis

WHITE PAPER

The Telecommunications Security Act Code of Practice

The TSA and Your Identity Infrastructure

TABLE OF Contents

Introduction

Telecommunications—encompassing landline and mobile phone services, internet, radio, television, and satellite services—is a key sector in every digital society. Other critical national sectors—such as healthcare, defence, and energy—rely on telecoms for their operations.

Cybersecurity threats towards the telecom industry are increasing in both prevalence and impact. Numerous attacks across the UK and internationally have garnered global notoriety. Some, targeting Dixon Carphone warehouse, Verizon and T-Mobile,[1] as well as AT&T,[2] were perpetrated by criminal crime groups while others are linked to nation states—such as Salt Typhoon's successful attack on multiple U.S. telecoms in 2024,[3,4] Kyiv Star in 2023,[5] and an attack on the UK Domain registry Nominet.[6]

In 2021, recognising the danger these threats present to public safety and national security, the UK Parliament established a new security framework: the Telecommunications (Security) Act.[7]

The TSA is intended to address both nation-state and criminal attacks for financial gain against telecom organisations by requiring large and midsize operators (categorized as Tier 1 and Tier 2 providers) to manage cybersecurity risk and security compromises to public electronic communications networks and services.

The 2021 TSA adds multiple cyber resilience requirements to the 2003 Communications Act and covers telecommunications in England, Wales, Scotland, and Northern Ireland. To achieve compliance, operators must establish protective capabilities, respond to cyber events, and report on them in a timely matter.

The regulatory framework for the TSA went into effect 1 October 2022[8] for operators of public telecom networks and services and established stiff potential penalties for non-compliance with the act and its Code of Practice. Daily fines as high as £100,000 or £10 million overall can be imposed and enforced by the UK's telecommunications regulator, Ofcom.

---

1 T-Mobile, Verizon workers get texts offering $300 for SIM swaps
2 AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records | WIRED
3 Exclusive | Chinese-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack - WSJ
4 White House links ninth telecom breach to Chinese hackers
5 Ukrainian cellular and Internet still out, 1 day after suspected Russian cyberattack - Ars Technica
6 UK domain registry Nominet confirms breach via Ivanti zero-day
7 Telecommunications (Security) Act 2021
8 The UK Telecoms (Security) Act | NCC Group | Leading Cyber Security & Managed Services

The Telecommunications Security Code of Practice

TSA sections 105E and 105F detail required security measures based on recommendations from the National Cyber Security Centre (NCSC).[9] These are outlined in a sector-specific guidance document, the Telecommunications Security Code of Practice,[10] drafted and issued by the Department of Digital, Culture, Media and Sport (DCMS).

The regulations and Code of Practice relate to providers of public electronic communications networks or services.[11] Since the issuance of the Code of Practice, elements of this comprehensive document have been elevated into law by the Electronic Communications (Security Measures) Regulations 2022,[12] which also enhances the original Communications Act 2003.

Timelines for compliance

TSA requirements were phased in based on provider tiers. For Tier 1 providers (with revenues over £1bn), the first iteration of requirements came into effect in March 2024. Tier 2 providers (with revenue over £50mil) had until March 2025 before they were required to comply with the Code of Practice.

Further controls come into scope in 2026, 2027, and 2028.

Identity security and TSA compliance

The TSA requirements detailed in the Code of Practice are comprehensive, covering security risk management, security architecture, security of management plane, networks, and specific security capabilities.

If you're the person responsible for identity security in your organisation, you must consider how your identity system supports security of different domains:

- Corporate domains
- Network oversight functions
- Management plane
- Central and decentralised network functions
- Security critical functions

9 National Cyber Security Centre - NCSC.GOV.UK

10 Telecommunications Security Code of Practice

11 As defined in section 151 of the Communications Act 2003 https://www.legislation.gov.uk/ukpga/2003/21/section/151

12 The Electronic Communications (Security Measures) Regulations 2022

The interdependent nature of these operational functions makes securing the identity systems themselves a security-critical function.

The 150-page Code of Practice covers the TSA's required cyber-resilience capabilities, which align to internationally recognised security management processes, including:

- Management of assets and risks
- Protection of services
- Monitoring and detection of threats
- Incident response and recovery of regulated services

Through decades of experience protecting, defending, and restoring identity systems before, during, and after cyber crises, we've gained a deep understanding of how identity systems contribute to the security of critical infrastructure and services.

Let's explore why the security and resilience of your identity systems are vital to accomplishing the objectives of the TSA regulation and its Code of Practice—and consider the steps you can take to achieve operational resilience.

Asset and risk management

The TSA regulation views security risk from multiple angles. The identity system is an asset that needs to be protected; and Active Directory (AD) and Entra ID identity systems are security-critical functions that potentially impact the resilience of different security zones, including the corporate environment, the management plan, the network, and customer equipment.

TSA Code of Practice reference	Implications for organisations
Sections 2.64 and 2.65 address visibility to host pools (system segments categorized by type and risk level), taking a technical approach to asset management. Know the attributes of a host or device as well as the state and security characteristics of all assets.	Your organisation needs to be able to identify assets that could be impacted by cyber risks. As a provider, you need to understand the segregation of your systems and assets, be able to identify interdependencies across the security architecture, and know which systems and assets are security-critical functions.
Section 10 addresses Regulation 11 requirements, which specify providers must conduct regular reviews of their security measures, "taking into account relevant developments relating to the risks of security compromises occurring."	Ensure you have a strong grasp of your security risks and visibility to threats across the network and supply chain, with specific focus on security-critical functions.

The Code of Practice takes a technical approach to asset management, so providers need clarity on:

- The devices and hosts that are part of their operations
- The specific roles they play in the resilience and security of the network
- How they relate to the processes and capabilities of the business

The risk management approach incorporates ongoing and annual formal risk assessments, reinforced with additional scanning and testing. In the case of your identity systems, it's essential to understand the capabilities they support and their role as security-critical functions.

You will need extra security capabilities, segmentation, and preventative, detective, and responsive controls. You also need clarity on how your identity system infrastructure acts as a dependency for key assets in all your domains, including the corporate, network, and security functions.

Key activities for identity system risk management

- Confirm your asset management programme is in place and you have firm control over your on-premises and cloud identity management services and their dependencies.
- Establish a security risk management programme based on a comprehensive standard.
- Ensure you understand the security risks associated with your on-premises and cloud identity systems, including risks associated with loss of integrity, confidentiality, or availability of the services.
- Understand and mitigate downstream impacts on other technology-driven services in the case of a compromise or outage of your identity systems.

Vulnerability management and attack surface reduction

The TSA Code of Practice emphasises the importance of protecting security-critical functions by managing and mitigating vulnerabilities and taking steps to reduce the overall attack surface. Section 12 sets out a clear competency requirement:

> *"...to ensure that the equipment is set up according to a secure configuration approved by appropriately trained security personnel, following procedures which enable it to be demonstrated that the configuration has been carried out in that way."*

Globally, cybersecurity vulnerabilities continue to multiply. The NCC Group reported an increase from just under 30,000 in 2023 to more than 40,000 in 2024. Only a small number of these is actively exploited, but certain areas such as perimeter devices constitute a key vector of initial access for malicious actors.[13] As an example, Emsisoft reported that nearly 3,000 organisations were breached with the zero-day vulnerability in the file transfer tool MOVEit.[14] Meanwhile, the Chinese state threat actor Salt Typhoon made great use of vulnerabilities in a variety of commercial off-the-shelf products such as Cisco IOS in their 2024 and 2025 campaign against U.S. and international telecoms.[15]

TSA Code of Practice reference	Implications for organisations
Sections 1.8 and 1.9 identify vulnerability management (including regular patching when updates are available) and attack surface reduction as essential oversight functions. These requirements are repeated in several sections throughout the TSA regulation and the 2022 Electronic Communications (Security Measures) Regulations document.	Your identity systems are key sources of vulnerabilities and exposure. Threat actors will leverage any opportunities, often chaining initial access vulnerabilities with identity system vulnerabilities for privilege escalation, lateral movement, and persistence in the environment. Identity security is a foundational capability to secure any telecom operator network.

Vulnerability and attack surface management for large-scale operators are significant undertakings and the Code of Practice devotes significant focus to these requirements. Although the regulation is flexible enough to allow for risk-based decisions, operators are required to manage potential exposures on an ongoing and timely basis.

Your identity systems support most of your critical IT-enabled capabilities, so rapid identification and mitigation of vulnerabilities as well as ensuring secure configuration is essential.

Key activities for identity attack surface management

- Establish a vulnerability management and mitigation programme, setting a policy for continually assessing indicators of exposure and compromise in your identity systems.
- Overlay this information on your asset management capability, focusing on critical services, security-critical functions, and internet-facing capabilities.
- Establish a remediation programme and prioritise mitigation of your identity vulnerabilities and indicators of exposure.

13 Cyber Threat Monitor Report 2024 | NCC Group
14 Unpacking the MOVEit Breach: Statistics and Analysis
15 China's Salt Typhoon Spies Are Still Hacking Telecoms—Now by Exploiting Cisco Routers | WIRED

- For identity security posture management, prioritise remediation of your indicators of exposure, starting with all Critical, High, and Medium severity findings. Rank findings in each category from the easiest to most difficult to remediate.
- Build an operating system patch management process focusing on remediation of identified vulnerable-but-critical services and their high-impact vulnerabilities.
- Apply just-in-time and privilege access management practices to individuals responsible for vulnerability remediation and patch management.

Reliable and resilient identity and access management

The Code of Practice relies heavily on identity and access management (IAM) as a means of achieving resilience. IAM enables critical controls for ensuring data security, reliable monitoring, secure backups, and secure administration.

Identity and access risks remain some of the main threat vectors for organised crime, which regularly leverages password spray attacks and weak passwords,[16] excessive or misconfigured permissions,[17] and vulnerabilities in multifactor authentication (MFA) configuration to give attackers the dreaded way in. In 2024, Microsoft reported 7,000 identity-based attacks per second, 99% of them focused on passwords, up from 4,000 the year before.[18]

Because telecoms often manage the "fuel" for MFA controls through SMS messages used for identity verification, many threat actors, such as Octo Tempest/Scattered Spider, have targeted operators as a way of enabling focused cyberattacks or broader hacking campaigns at scale.[19]

TSA Code of Practice reference	Implications for organisations
Sections 6.10 requires public telecom providers to retain control of day, leveraging authentication and authorisation methods including MFA. **Section 7.2** details Regulation 8, which requires controls to prevent unauthorized access or changes to systems, credential management, identity management, and implementation of a least privilege access model.	IAM regulations are highly complex, covering corporate, management environment, and the networks themselves. You will need a strong fundamental security architecture and a variety of IAM controls that depend on a secure identity infrastructure, whether on premises or in the cloud.

16 No or weak credentials is the lead compromise factor with 47.8% according Google Cybersecurity Action Team, Threat Horizons, Apr 2023

17 Palo Alto Unit 42 found that 99% of cloud users, roles, services, and resources are granted excessive permissions

18 Microsoft Digital Defense Report 2024

19 T-Mobile, Verizon workers get texts offering $300 for SIM swaps

Any misconfiguration or vulnerability in your on-premises, cloud, or hybrid identity infrastructure could provide an attacker with the opportunity to compromise foundational security controls and open a direct path to disrupt critical capabilities or services.

AD and Entra ID are complex systems needing deep experience, strong skills in configuration and operations, continuous monitoring for indicators of exposure and compromise, and instant response to incoming attacks. Managing such a foundational capability is difficult at scale and will require automation.

Key activities for IAM

- Implement a least privilege access model so only specific roles have the privileges needed to perform high-privilege functions.
- Establish a programme to monitor indicators of exposure and compromise and identify staff with specialised expertise to continually assess and remediate these.
- Implement just-in-time and privileged access management principles to safeguard your most sensitive accesses (also known as Tier 0)—especially AD, which should always be considered a Tier 0 asset.
- Review the Entra ID Connect synchronisation rules to be sure proper segregation of access exists between AD and Entra ID. Synchronize only the necessary principals for Entra ID services.
- Regularly execute active penetration testing, red-teaming, or full incident response tabletop exercises to ensure the identity infrastructure is secure. These measures can provide you with assurance of your identity system's security posture and resilience.
- Ensure detection, logging, and reporting are in place for threat hunting.
- Invest in automation of scanning, detection, and remediation of vulnerabilities, exposures, and compromise of the identity system.

Business continuity management

To achieve the level of service resilience that the TSA requires, make sure you can recover your systems quickly to a stable and trusted state in the event of an outage or breach.

TSA Code of Practice reference	Implications for organisations
Section 1.11 directs providers to operate in a state of "assumed compromise," in which it is understood that attackers have already infiltrated operations and can execute an attack at any time. **Sections 2.50, 2.51, and 2.52** underline the importance of ensuring you can restore services securely to a known-clean state, first isolating the restored systems and performing forensic analysis to ensure that malware is not present and that attackers are not able to persist in the environment. **Regulation 9** goes into more detail, requiring offline backup and restore of critical services to enable security teams to ensure the restore doesn't reintroduce malware, helping to limit adverse effects of security compromises.	Your identity infrastructure is a highly complex capability with many interdependencies. Identity is a core foundation of your technology-enabled services and restoring AD is a complex, high-risk operation. Comprehensive planning and regular testing of your restore capabilities is essential if you want to be able to rely on them in a real-life cyber crisis.

Your identity infrastructure is the key to accessing most, if not all, digitally enabled services. Without a disaster recovery and continuity plan for AD and Entra ID, you are unlikely to be able to restore your services after a major destructive event.

Testing identity recovery can be a significant challenge due to the dependencies and challenges of full AD forest recovery. Microsoft's official forest recovery guide is a multi-step—often multi-day—process, and even a slight deviation can curtail a successful recovery.[20,21]

To compound the challenge even further, once AD is restored, it still can't be trusted without extensive forensic analysis to remove persistence mechanisms that the attacker uses to retain a footprint after restore. In addition, following a cyberattack, regulators will expect full reporting of the incident investigation and will require AD to be included in regular restore testing.

20 Active Directory Forest Recovery Guide | Microsoft Learn

21 Top Manual AD Forest Recovery Pitfalls | Semperis Guides

Key activities for identity system continuity

- Define a plan for identity infrastructure recovery and restore, designating responsibility for specific recovery tasks to qualified team members.
- Confirm measures to ensure clean-state recovery, including immutable, air-gapped backups.
- Establish an out-of-band crisis response plan and test environment and perform frequent restore testing.
- Ensure identity system disaster recovery activities are implemented and integrated with your overall business continuity and crisis management plans and exercises.

Monitoring and detection

Due to the high number of cyberattack techniques that focus on AD,[22] monitoring and detection becomes key to resilience and containment.

TSA Code of Practice reference	Implications for organisations
Regulation 6 deals with all aspects of monitoring, including what to monitor, coverage expected, detection and analysis of anomalous activities, and implementing immediate alerts and mitigation of those activities—using automation where possible. The 2022 Security Measures Regulations further reinforces these guidelines in law. **Sections 1.13 and 1.14** require continuous, real-time monitoring of security-critical functions to establish a baseline of normal activity, quickly detect anomalies, and enable quick response to any exploitation.	To effectively execute on the requirement for active cyber protection, you must have effective cybersecurity monitoring and detection in place. Map your organisation's critical services and establish continuous, real-time logging and monitoring of those services, including the identity infrastructure.

When thousands of users—and non-human (machine) identities—operate across your network, corporate, management domain, and critical services, it is vital that you have logging in place and appropriate detection of unusual behaviours, malicious actions, and unexpected changes.

Achieving this level of constant attention requires a multitude of actions, ongoing review of configurations, and hardening of your identity systems. Automation is essential and should be integrated with and managed by a team with the specialised skills required to respond to any potential or suspected incidents.

22 NSA Jointly Releases Guidance for Mitigating Active Directory Compromises > National Security Agency/Central Security Service

Key activities for monitoring the identity system and detecting compromise

- Configure and manage proven, industry-recognised security measures on your identity system.
- Ensure logging is enabled and a trained team is monitoring for suspicious and potentially harmful events.
- Enable secured logs on your identity infrastructure to ensure logging can't be compromised or encrypted.
- Consider identity-focused analytics tools for a richer data set and scalability through automation.

Incident response and forensics

The TSA regulation imposes significant requirements on operators for incident response and management.

TSA Code of Practice reference	Implications for organisations
Regulation 10 details measures for incident response and readiness, including creating a plan and policies for managing security incidents, establishing clear channels for communicating identified threats and responding to incidents, and reporting risks and incident responses to appropriate governance personnel. The 2022 Security Measures Regulations further reinforces these guidelines in law.	You need to have a comprehensive view of your organisation's security posture—before, during, and after an incident. Early identification of threats and compromise can help contain a cybersecurity incident and reduce its adverse effects. But to achieve this level of effectiveness, you must have plans, policies, and process in place—and tested—to manage incidents and report on them to regulators and other stakeholders. Additionally, visibility and integrity of identity system logs is essential for meaningful forensic analysis.

AD forensics are challenging. Attackers strive to attain privileged access; once they have it, they have broad powers to delete audit logs, implant malware, and establish persistence in the environment. This makes them hard to detect—and harder to remove.

Numerous threat actors, such as RansomHub, LockBit, and Ghost, have all made effective use of such techniques.[23]

Key activities to ensure prompt, effective incident response

- To understand your risk profile, conduct a thorough security review and map attack pathways leading to Tier 0 assets—especially the identity system—including deep analysis of shadow administrators, nested groups, and local administrative rights.

23 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-050a

- Provide your security team with clearly defined playbooks for different levels of escalation and procedures for each type of cyber incident.
- Devise an incident response plan that includes clearly defined roles for each member of your team and their responsibilities during incident response.
- Ensure the integrity of your identity system logs and establish the ability to monitor and reverse changes in AD in near-real time.
- Establish an ability to collect forensically sound data on your identity system and perform a forensic investigation to determine the origin and methods of attack.
- Ensure your identity forensics capabilities are integrated and tested as part of your broader incident response readiness.

Tool specialisation

Unlike many other cyber resilience regulations, the TSA and associated Code of Practice are highly industry specific but also multifaceted. The regulation deals with abstract technical concepts and includes a variety of focuses on zones, security architectures, security-critical services, and more.

Translating these into technology- and service-specific measures is a major undertaking. For complex technologies, such as identity systems, the challenge is even greater. Managing identities and access is a job that already keeps most operations teams more than busy. Securing and monitoring identity systems to comply with the TSA just adds more work for your team.

To help create focus and capacity for such teams to reduce security risk, consider evaluating solutions that are purpose-built for identity security. Semperis offers both free and paid tools that directly address the challenges of complying with the TSA where those measures matter most—in the identity system.

Let's take a look at the specialised capabilities that Semperis provides to help you address TSA requirements.

How can Semperis help?

Challenge	How Semperis can help	Solution
Risk management To comply with the TSA, it is vital that you drive your security risk management from a foundation of robust asset management. Additionally, you must manage your identity system status as a security-critical function.	• Map threat and vulnerability indicators in AD and Entra ID. • Provide visibility into identity security posture. • Provide ongoing risk identification and management.	• Active Directory Forest Recovery (ADFR) can map and automate forest recovery, including relevant dependencies. • Purple Knight (community tool) provides point-in-time AD security assessment and recommends fixes for indicators of exposure and compromise. • Directory Services Protector (DSP) provides comprehensive tracking, capturing every change made in AD and helping identify and roll back malicious changes.
Vulnerability management and attack surface reduction It is vital to be able to identify, prioritise, and mitigate vulnerabilities and indicators of exposure.	• Deliver semi-automated, research-led view of software vulnerabilities and misconfigurations. • Provide point-in-time vulnerability and misconfiguration scanning. • Enable continuous, automated vulnerability and misconfiguration scanning.	• Lightning Intelligence provides clear security posture insights across hybrid AD and Entra ID environments in an easily deployed SaaS solution to simplify security posture assessments. • Purple Knight provides point-in-time AD security assessment and recommends fixes for indicators of exposure and compromise. • DSP provides continuous threat and vulnerability detection automated rollback of risky and malicious changes.

Challenge	How Semperis can help	Solution
IAM and privileged access Establishing strong identity and access controls helps you ensure robust identity and technology resilience.	• Provide privileged access management and identity and access management for all users. • Enable multifactor authentication independent of Privileged Access Workstations (PAW). • Enhance protections for security-critical functions, including your identity infrastructure, supporting regulated services in ensuring confidentiality, integrity, and availability.	• DSP enables continuous monitoring of AD and Entra ID security posture, ensuring the underlying identity systems are secure and trustworthy. • Forest Druid (community tool) discovers attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit. • Forest Druid supports AD teams in mapping attack paths automatically.
Business continuity management To comply with the TSA and Code of Practice, you need to be able to restore your identity infrastructure rapidly to a known clean state—and have testing that proves you can.	• Enable early detection or avoidance of a security breach of your identity system and dependent technology-enabled services. • Provide proven, clean-state restore with validated recovery objectives. • Operationalise proven crisis and incident response frameworks, enhanced with expert playbooks—from preparation to after-action review.	• ADFR can automate forest recovery, restoring AD quickly and safely without reintroducing malware. • ADFR automates the complicated recovery process and reduces AD recovery time by up to 90%. • ADFR also allows for post-breach forensics to identify persistence and recover AD to a trusted state. • Disaster Recovery for Entra Tenant (DRET) recovers Entra ID objects. • Ready1 centralises crisis response, enabling teams to develop, test, remediate, and continuously improve incident response planning.

Challenge	How Semperis can help	Solution
Monitoring and detection Your identity infrastructure is a rich source of vulnerabilities and misconfiguration, requiring skill and dedication for meaningful detection.	• Provide AD and Entra ID monitoring to detect attacks and enable accurate incident reporting. • Comprehensively control the constantly changing AD environment with its rich attack surface. • Provide visibility into AD-focused attacks and changing vulnerabilities.	• DSP provides continuous threat and vulnerability detection, capturing every change made in AD, helping identify malicious changes, and automatically rolling back risky changes. • Forest Druid discovers attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit. • Identity Runtime Protection uses machine learning to perform attack pattern detection by capturing, analysing, and correlating AD user activities with Semperis' identity threat intelligence to signal malicious behaviour.
Incident response The TSA imposes strict incident reporting requirements on organisations.	• Secure your logs for forensic analysis. • Enhance ability to detect actions of a malicious actor and rapidly report incidents and attacks impacting AD and Entra ID.	• DSP provides comprehensive logging and highly specialised AD and Entra ID threat analysis, enabling up-to-date and industry leading insights and enrichment of SOC visibility through SIEM integration. • Identity Runtime Protection utilises machine learning to perform attack pattern detection by capturing, analysing, and correlating authentication activities with Semperis' identity threat intelligence to signal malicious behaviour. • Ready1 centralises and unifies all aspects of cyber crisis planning and incident response, ensuring seamless crisis response through preparation, collaboration, and enterprise-wide communications.

Conclusion

The Telecommunications Security Act and the associated Security Code of Practice is a major step up in security and resilience requirements for UK telecom providers. To comply with the regulation, we recommend you establish six major capabilities for the resilience of your AD and Entra ID services, including:

1. Establish a programme for risk management and ownership of your identity system resilience.
2. Establish a comprehensive and automated exposure, threat, and vulnerability monitoring programme and integrate this capability to your security operations centre.
3. Reduce the attack surface of your AD and Entra ID infrastructure through the continuous monitoring for indicators of exposure and compromise. Build and maintain a programme that continually assesses vulnerabilities and empowers timely remediation.
4. Build a tested incident response capability for your technology services and security-critical services, including your identity system, to enable rapid incident response, reporting, and forensic capabilities.
5. Develop an automated and tested recovery process to enable rapid restore of your identity system to a proven clean, stable, and trusted state.
6. Establish a project of continuous improvement, including best practices from established experts in the cybersecurity industry.

In our experience, achieving these capabilities is challenging, and sustaining them over time is not possible without significant automation. Semperis' market-leading products and services can provide you with this threat-led, automated capability.