Magrathea Telecommunications Limited,
5 Commerce Park, Brunel Road, Theale,
Berkshire RG7 4AB

0345 004 0040 info@magrathea-telecom.co.uk

Guidance on the UK Telecommunications Security Framework

Contents

This document is for clarity and guidance but does not seek to replace official regulations or guidance and all Service Providers are responsible for satisfying themselves that they are adhering correctly to current standards and rules. Magrathea accepts no liability whatsoever for any errors, omissions or statements in this guidance or for any loss which may arise from your use of this guidance.

This guide is prepared for communication providers with a turnover of less than £50m. If your business has a turnover in excess of that you will be classified as Tier 1 or Tier 2 and should contact us directly for specialist advice on next steps.

Aims of The Telecoms Security Framework and who needs to comply

High level aims of the security and resilience regulations

With such a complex set of regulations and interpretations it is important to keep in mind the spirit of the requirements. The overarching aims and duties are to:

- Identify the risks of security compromises
- Reduce the risks of security compromises occurring
- Prepare for the occurrence of security compromises

A 'security compromise' includes anything that impacts availability, performance or functionality including loss of signals, alteration of signals or exploitation. So, this could include malicious acts as well as run of the mill network outages.

Telecoms Security Framework

To help put the guidance into context here is a brief overview of each element that makes up the framework.

Layer 1	The Communications Act 2003 and The Telecommunications (Security) Act (TSA) (https://www.legislation.gov.uk/ukpga/2021/31/introduction)	The TSA came into force in October 2022 and amends the Communications Act 2003, giving extra powers to Ofcom and imposes additional duties on all telecom providers in relation to security controls within their organisations and that of key suppliers.
Layer 2	The Electronic Communications (Security Measures) Regulations 2022 (https://www.legislation.gov.uk/uksi/2022/933/contents)	These regulations support the TSA by providing a set of detailed measures expected to be put in place by telecom providers and networks. 'Micro-entities' are exempt[1]
Layer 3a	Security Code of Practice (https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf)	This document, created by DCMS, is intended to provide clarity on how to achieve compliance with the regulations. It does not apply to Tier 3 or Micro-entities although Tier 3 providers may find it useful to help meet their obligations.
Layer 3b	Network and Service Resilience Guidance for Communications Providers (https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/272921-resilience-guidance-and-mobile-ran-power-back-up/associated-documents/network-and-service-resilience-guidance-for-communication-providers.pdf?v=375122)	This document, created by Ofcom, is intended to set out the general approach which Ofcom would normally expect providers to take to comply with the resilience related duties under the Comms Act and is applicable to all sizes of Comms Provider. This should be read alongside the Security Code of Practice which covers cyber-security more specifically.

[1] Micro-entities must satisfy two or more of the following: turnover of £632,000 or less, balance sheet total not more than £316,000 and no more than 10 employees. The full definition can be found here: https://www.legislation.gov.uk/ukpga/2006/46/section/384A

Who has to comply with the regulations

The regulations (Layer 1) generally apply to all providers but in order to take a proportionate approach to compliance, the Code of Practice has been split into a tier system. Three tiers have been created based on turnover and mirror those used to determine Ofcom administrative fees. These tiers are:

Tier 1	Public telecoms providers with relevant turnover in the relevant period of £1bn or more
Tier 2	Public telecoms providers with relevant turnover in the relevant period of more than or equal to £50m but less than £1bn
Tier 3	Public telecoms providers whose relevant turnover in the relevant period is less than £50m, but who are not micro-entities[1]

Tier 3 providers are not expected to follow measures within the Security Code of Practice (Layer 3a), however it is acknowledged that they may wish to do so where it is appropriate and proportionate in order to satisfy their obligations under the regulations.

Micro-entities (typically providers with a turnover below £632,000) are exempt from the specific regulations listed in Layer 2 and therefore the Security Code of Practice itself does not apply to those either.

> *Remember: Only micro-entities are exempt from the regulations, all other providers must comply with Layer 1 and Layer 2 but do not have to follow the Code of Practice to do so! The Code of Practice gives guidance for Tiers 1 and 2, guidance for Tier 3 may be issued at a later date.*

In all cases it is important to note that, if you provide services to a provider in a higher tier, they are likely to require you to meet the standards necessary in that tier in order for themselves to be compliant.

What if you don't comply

Ofcom are responsible for regulating the security framework and will monitor compliance. They have powers to request information in order to do so and can issue contravention notices, initiate enforcement action and issue fines.

The document lays out what measures need to be in place by which date, and how to test your readiness. Ofcom and the NCSC are available to support your journey to compliance.

The remainder of this document assumes you are a Tier 3 provider or micro-entity who needs to ensure compliance with the Communications Act and the TSA, including the General Conditions of Entitlement.

Our aim is to highlight the key areas you most likely need to address and signpost you to useful resources. We cannot offer detailed or personalised guidance. It remains your responsibility to ensure compliance with all legal and regulatory requirements.

Overview of the key areas of the Security Framework

Electronic Communications (Security Measures) Regulations 2022

These regulations support the TSA by providing a set of detailed measures expected to be put in place by telecom providers and networks. 'Micro-entities' are exempt but anyone with turnover of over £632,000 must be able to show compliance.

The term 'security compromise' covers "anything that compromises the availability, performance or functionality of networks and services" and "anything that causes signals conveyed by means of the network or service to be lost" (as defined in section 105A of the Communications Act).

The key parts of the regulation can be briefly summarised as follows:

Network architecture: A network provider must design and construct networks in a manner which reduces the risks of security compromises occurring, existing networks are to be redesigned.

Protection of data and network functions: A network provider must use technical means that are appropriate and proportionate to protect data stored in relation to the operation of the network and to protect the functions of the network.

Protection of certain tools enabling monitoring or analysis: Where tools to enable monitoring or analysis of the network are located outside of the UK, the network or service provider must identify and reduce the risk of security compromise as a result of being outside of the UK.

Monitoring and analysis: A network provider must take appropriate and proportionate measures to monitor and analyse the operation of security critical functions, using automated means where possible, and to investigate anything unexpected or unusual.

Supply Chain: Providers must take proportionate and appropriate measures to identify and reduce the risk of security compromises as a result of things done or omitted by third party suppliers.

Prevention of unauthorised access or interference: Providers must take appropriate and proportionate measures to reduce the risk of security compromises that consist of unauthorised access to the network.

Preparing for remediation and recovery: Providers must take appropriate and proportionate measures to prepare for occurrences of security compromises with a view to limiting the adverse effects of such compromisers and enable the provider to recover.

Governance: Providers must ensure appropriate and proportionate management of people that have been given the responsibility for taking the measures to comply with regulations.

Reviews: A provider must undertake regular reviews of measures in place and review the risks of a security compromise occurring at least once each year.

Patches and updates: Where a software or equipment provider makes a patch or mitigation available relating to the risk security compromises, providers must deploy within an appropriate time frame.

Competency: Providers must take appropriate and proportionate measures to ensure that people given responsibility for taking measures are competent and have the appropriate resources available to them.

Testing: Providers must carry out testing at appropriate intervals to identify risks of security compromise. Tests should be carried out where possible without warning to those responsible for identifying and responding to risks.

Assistance: Where a security compromise occurs that may cause a connected compromise the provider must provide information and assistance to the other provider.

Ofcom's Network and Service Resilience Guidance

This resource is aimed at ALL providers, including Micro-entities, and for those in Tiers 2 and 3 should be read alongside the Security Code of Practice which focusses much more on cyber security matters.

The guidance, updated in September 2024, offers good practice in the design and operation of networks and services in relation to resilience and security and will help with compliance of the Communications Act 2003.

The guidance is not the only way to be compliant, however where a different approach is taken Ofcom will expect providers to be able to explain the reason for the alternative.
The key measures include:

- Ensuring that networks are designed to avoid or reduce single points of failure;

- Ensuring that key infrastructure points have automatic failover functionality built in so that when equipment fails, network traffic is immediately diverted to another device or site that can maintain end user connectivity;

- Setting out the processes, tools and training that support the requirements on resilience.

We highly recommend you review the guidance for the detailed measures which Ofcom suggest, meanwhile below we highlight some key points that we believe are relevant for the majority of our clients to be aware of and may be different from your current approach.

- Resilience obligations apply to you end to end, even if you don't control the entire path. It's important to work with suppliers who have a similar approach to resilience management, including carrying out regular reviews and joining understanding risks and management of those risks.

- Core network elements, or sites, are expected to be physically separate with diverse connectivity between them. They should also be able to survive power loss for at least five days.

- Interconnects and internet peering must have appropriate capacity to ensure reliability. Recognising that the general internet can suffer from abnormal or malicious traffic, providers are expected to monitor in order to perform appropriate traffic management.

- Interconnects that may carry critical traffic (e.g. emergency calls or calls to/from vulnerable people) should not rely on the general internet. Interconnects between networks are highly likely to carry essential calls and therefore should be separate from the internet. Utilising peering via an internet exchange is likely to be considered a reasonable alternative to physical direct interconnect.

- Management functions should be sufficiently segregated from production traffic (i.e. traffic created by your service) so they cannot impact each other. As a minimum, Ofcom suggest the use of different sub-networks such as VLANs.

- The sole use of 'in band' management is not recommended as it can result in being locked out of your service. Providers should consider 'out of band' management which is separate and not used for production traffic.

- 'Digital Landline' is a term introduced by Ofcom to convey the concept of a PSTN replacement service. Users of this service are likely to expect a high level of resilience and may rely on the service to make critical or emergency calls. With this in mind CPs must be careful to flag all and any potential risks when providing a service that could be considered a 'digital landline'. For example, by making it clear that power failures or problems with the internet connection could result in loss of service.

- 'VoIP' is an umbrella term but is often used in relation to 'Over the top' (OTT) services that are relying on the wider internet and Ofcom believe this delivery model is unlikely to be appropriate for services supplied to essential public service providers due to the increased resilience needs. Providers are expected to assess customer use requirements and where appropriate provide information any vulnerabilities and risks associated with using your service. This would include things like downtime due disruption to the internet connection, power outages and so on.

- In addition to the network and management tools, providers must consider:

    - Service level management: Ensure design can meet requirements

- Capacity management: Ensure sufficient capacity to cope with failures
- Availability management: Measure against service levels and address issues
- Continuity management: Be clear how risks will be managed and mitigated
- Supplier selection, management and spares: Assessments of suppliers, hardware and software to be based on testing resilience and reliability
- Change management: have a robust process in place to minimize impact on service availability
- Asset and configuration management: maintain records of assets and demonstrate understanding of the service impact if any asset fails
- Testing and validation management: Ensure new services or changes to existing meet required service levels
- Knowledge management: Gather, analyse, store and share knowledge within your organisation

Where process measures are implemented, there must be a clear line of responsibility and chain of command from the Board level down to operational delivery, with clear evidence of this in any relevant internal documentation.

- Service Operation relates to the day-to-day management of a service, including shared services and outsourced aspects of the service or network. Processes that relate to this obligation are:
  - Network Control-Plan Monitoring: Ingress and egress points should be monitored
  - Network User-Plan Monitoring: Monitoring for capacity planning and faults
  - Event Management: Infrastructure and services to be constantly monitored
  - Incident Management: Manage the lifecycle of incidents including logging, reporting and escalating as necessary
  - Problem Management: Minimise adverse impact by preventing incidents from occurring, or prevent recurrence
  - Operations Centres and Help Desks: Establish centres to support continuous monitoring. Where an incident may cause disruption to another network or service, the provider must provide assistance.

- The guidance mentions knowledge and expertise throughout but specifically states that providers are expected to take measures to ensure that "responsible persons have appropriate knowledge and skills to perform their responsibilities effectively" and the provider is expected to ensure their staff, or others acting on their behalf, are suitably qualified.

- Where network automation is used, such as deployment, testing or monitoring, it can have great benefits but also introduces risks. To mitigate the risks providers are expected to take measures to ensure that they apply an appropriate level of diligence when implementing network automation.

For the purposes of this summary we have focussed on guidance that will impact typical 'over the top' voice service providers. If you have physical infrastructure or a complex supply chain we strongly encourage you to review the referenced documents for additional areas that might impact

What is expected of our clients to meet the requirements of the framework

The scope of the measures include "the systems and services involved in providing public telecommunications services to customers" so the TSR applies to the majority of our clients. Even if a client considers themselves a micro entity, if telecom services are provided, especially to a vertical which is critical or vulnerable e.g. NHS, Care homes, etc. then we would advise that as a minimum there is an understanding of the regulations and reasons understood if and why measures are not adopted at all.

Whilst smaller clients are not expected to follow the measures in the Security Code of Practice to the same degree as Tier 1 & 2 providers, they **may** choose to adopt the measures included within the code of practice where these are **appropriate and proportionate** to their networks and services.

The use of the word 'may' here indicates that clients are likely to have multiple options, all of which could deliver a satisfactory solution to meet the measures and there are likely to be differences between providers in their implementation.

The phrase 'appropriate and proportionate' is mentioned at least 38 times in the Code of Practice so this implies an expectation that all providers are required to adopt the appropriate measures to a degree, all be it in a way that works practically for their business

If there is a decision taken within your business not to adopt any of the measures in the Code of Practice, when investigating any issues Ofcom, will expect to see reasons why alternative actions were taken instead. Fines can be issued for non-compliance to these regulations and no-one wants to be in that position.

How Magrathea can support clients meet the requirements of the framework

It is expected that our clients already have processes and procedures in place to ensure their business operations and services are physically and cyber secure and that you have suitable disaster recovery plans. This is not about re-inventing the wheel but ensuring that everything already in place meets the requirements and identify any areas for improvement.

Documenting everything is important so that it can be regularly reviewed and audited. If ever there is a need it is also important to be able to present the documentation to Ofcom.

The following section utilises the key parts of the Electronic Communications (Security Measures) Regulations to cross reference how Magrathea's products and services can support clients with compliance.

Network architecture A network provider must design and construct networks in a manner which reduces the risks of security compromises occurring, existing networks are to be redesigned.	We can provide you with diagrams and information to show how we have minimized single points of failure within our network and where it is not possible to avoid a SPOF, what actions we take to mitigate impact. In addition, we offer a number of services that can support our clients improve resilience within their own operation, including: • Chargeable Number Translation Service: Allows fully flexible call routing to enable redirects and alternative features. • SIP Resilience: Allows you to nominate multiple end points for automatic failover and load balancing. • Backup Switch: Allows you to nominate a secondary endpoint to be used for disaster recovery when automatic detection is insufficient. • Direct Interconnect: Allows you to ingress and egress traffic directly between the two networks. • Co-location: A value-added service enabling clients to physically locate their equipment with ours in a secure location. • VPN Voice: Allows you to securely exchange traffic with Magrathea in a resilient way.
Protection of data and network functions A network provider must use technical means that are appropriate and proportionate to protect data stored in relation to the operation of the network and to protect the functions of the network.	The identification of potential risks and threats, whether through human or digital error or deliberate action to cause harm, requires proactive intervention and monitoring. Magrathea encrypt all end user data and store historic records securely with appropriate redaction to satisfy data protection rules. We provide encrypted call records and reporting and our new portal supports 2FA. Advice and guidance for clients on how to avoid fraud can be found here. This area also covers physical protection of critical assets from fire, flood and burglary. Our resilience products, particularly Co-location, can also help clients with this aspect.
Monitoring and analysis A network provider must take appropriate and proportionate measures to monitor and analyse the operation of security critical functions, using automated means where possible, and to investigate anything unexpected or unusual.	Security monitoring fundamentally underpins the security of a system. Inadequate coverage of devices from a logging and monitoring perspective will fundamentally limit the ability to identify, and subsequently determine the root cause of anomalous activity and may also limit the ability to understand the extent of such activity without recourse to extremely labour intensive and expensive forensic work. Magrathea continually monitors and analyses activity on our network and within our operations so clients can be assured that as a supplier we are fulfilling our obligations. When issues are detected relating to individual client accounts, clients are notified as a matter of urgency to enable full investigation with our support. Where feasible monitoring is automated and 24/7, more bespoke analysis is performed by our skilled team of support engineers.

Supply Chain Providers must take proportionate and appropriate measures to identify and reduce the risk of security compromises as a result of things done or omitted by third party suppliers.	This point focuses on the identification of risks from using 3rd party suppliers and putting in processes to mitigate those risks. Magrathea is a privately owned and managed business with full ownership of our core network and independent from any other network or service provider. Where we have partner, supplier or customer relationships such as carrier interconnect, number portability or hardware provision we carry out a 3rd party supplier risk process in order for us to identify and mitigate any risk and to agree monitoring and reporting procedures. Clients should take similar steps when assessing their relationship with Magrathea and we can provide a ready completed supplier summary on request, or are happy to answer your questionnaire to satisfy this obligation.
Prevention of unauthorised access or interference Providers must take appropriate and proportionate measures to reduce the risk of security compromises that consist of unauthorised access to the network.	Clients are responsible for ensuring they have adequate password security, Magrathea offers guidance on how to avoid fraud which can occur from poorly managed password systems. See here for details. We also support our clients in ensuring their interaction with us is secure, using encrypted data and password protected access to portals.
Preparing for remediation and recovery Providers must take appropriate and proportionate measures to prepare for occurrences of security compromises with a view to limiting the adverse effects of such compromisers and enable the provider to recover.	Clients are responsible for ensuring they have a detailed recovery plan to be used in the event of a network disaster. A combination of in-house and Magrathea tools can be used to restore service in the event of a major event. Clients are encouraged to carry out their own assessment of remediate and recovery needs and, if standard Magrathea services aren't available to support specific concerns, they should engage with our team to investigate bespoke solutions.
Testing Providers must carry out testing at appropriate intervals to identify risks of security compromise. Tests should be carried out where possible without warning to those responsible for identifying and responding to risks.	Procedures and tools should be tested to ensure readiness. Magrathea carry out disaster scenarios to ensure the team know how to react in a real-life situation, if you would like our support when testing scenarios for your business we would be happy to have input or play a role.

Assistance Where a security compromise occurs that may cause a connected compromise the provider must provide information and assistance to the other provider.	Magrathea is actively engaged with a number of industry bodies as well as closely managed inter-operator relationships. In the event of a compromise all relevant parties are expected to work together to understand the impact and provide assistance to mitigate risk and restore service where appropriate. Clients are expected to engage in dialogue with us, and 3rd parties, in order to provide assistance and information.

If you would like to know more about these services please contact us as sales@magrathea-telecom.co.uk or find out more on The Guide via our Magic Portal.