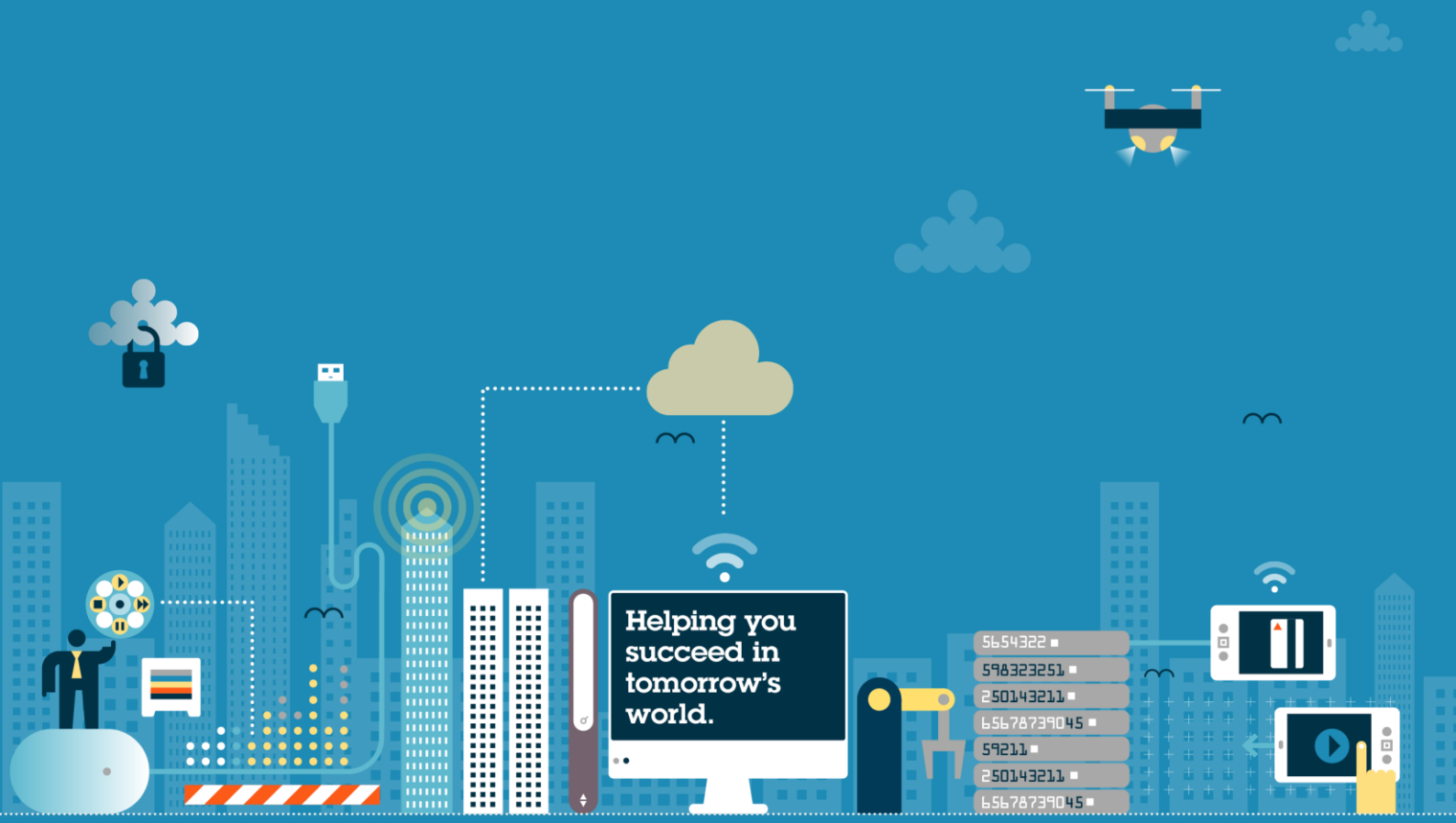
Telecoms Security Compliance

2024

Private & Confidential



Contents

01 Steps for a successful compliance project and how OC can support you

02 Security compliance checklist

03 Our team

The Telecoms Security rules put the UK at the forefront of the strongest rules for the sector in the world.

Introduced during 2021 and 2022 through the Telecoms Security Act, Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice, sees a step-change in the expectations on the communications sector with respect to assessing and reducing risks of security compromises on networks and services.

There is no one-size fits all approach to compliance, as what is considered 'appropriate and proportionate' will vary depending on both the size of your company and how it operates.

Providers with an annual revenue of over £50m will be classified as Tier 2 providers. Although the first implementation date set out in the Code of Practice is 31 March 2025, this is in recognition that it may take you longer to achieve compliance than a Tier 1 provider and therefore starting sooner rather than later will help you manage this.

Our six-step guide, and proposal set out in this document has been developed to help you kick off your Telecoms Security compliance project, and to show you how we can help (as much or as little as you like) along the way.

We would be delighted to be able to support you on understanding how the new telecoms security legislation will impact your business and the steps that are necessary to achieve compliance.

Our 6 step guide to a successful telecoms security compliance project

1. Lay the foundations

- Raise awareness and obtain senior level buy-in
- Review the legislation including the Telecoms Security Code of Practice
- Identify which Tier applies to your business
- Identify your priority areas of focus for compliance
- Allocate resource and budget
- Implement internal governance procedures
- Hold kick-off meetings

2. Take stock and gather information

- Identify which of your systems and operations are in scope
- Identify current security compliance measures
- Evaluate current compliance and procedures against new requirements
- Review your supply chain and assess security risk posed by these suppliers
- Don't rush this exercise

3. Pause, review and assess

- Review information gathered in step 2
- Perform 'gap analysis' to identify Telecoms Security Steps
- Build on any existing compliance frameworks
- Create your compliance 'roadmap'

4. Implementation

- Implement new policies and governance procedures
- Implement necessary technical changes
- (Re)allocate internal responsibilities
- Put in place processes for procedural compliance
- Review supplier contracts and prepare amendments (where necessary)

5. Finishing touches

- Take remedial steps identified as low risk
- Plan responses to any future changes in risks to security compromises
- Train your teams

6. Monitoring and maintenance

- Continue to monitor compliance and new threats to security that emerge
- Ensure annual reviews are undertaken and documented
- Provide regular updates to key stakeholders
- Plan and undertake regular 'fire drill' or 'war game' reviews of security incident management
- Monitor changes in revenue which could result in a change of tier
- Monitor changes to the Code of Practice (a review is scheduled in 2027)

Understanding your security compliance

The Telecoms Security Regulations are the overarching binding rules which your business must comply with. These are broken down into technical guidance measures in the Code of Practice.

We propose to break down the security compliance checklist into these categories of technical guidance.

Our support is best placed where there is a more legal or governance focus to the requirements. We have indicated in this table the areas that we recommend that we support you in:

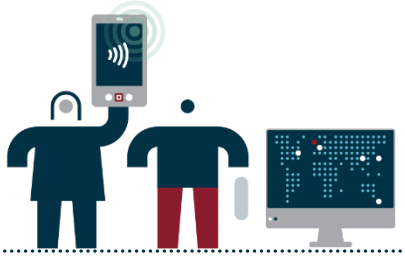
(a) Understanding the requirements by preparing a compliance checklist for you to complete

(b) Reviewing your responses to understand how your current practices align with the requirements. This will include interview-style workshops with you to understand your responses

(c) Preparing a gap analysis of current compliance against the new requirements

(d) Working with you to prepare a checklist and roadmap for remedial actions which are required

Technical Guidance categories	OC support
Overarching security measures	✓
management plane	✗
signalling plane	✗
third party supplier measures	✓
supporting business processes	✓
customer premises equipment	✗
virtualisation	✗
network oversight functions	✓
monitoring and analysis	✓



Our team

Hannah Drew
Legal Director
United Kingdom

T +44 20 7105 7184
hannah.drew@osborneclarke.com

Jon Fell
Partner
United Kingdom

T +44 20 7105 7436
jon.fell@osborneclarke.com

TK Spiff
Associate
United Kingdom

T +44 207 105 7615
tk.spiff@osborneclarke.com

Matt Suter
Senior Associate
United Kingdom

T +44 207 105 7447
matt.suter@osborneclarke.com