Security Conference 2022

Telecommunications (Security) Act 2021 Ofcom's role and regulatory approach

Gerry McQuaid

03/10/2022

Telecoms networks face a wide range of threats


The New York Times

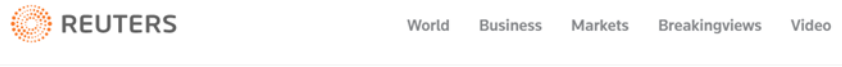
Burning Cell Towers, Out of Baseless Fear They Spread the Virus

A conspiracy theory linking the spread of the coronavirus to 5G wireless technology has spurred more than 100 incidents this month, British officials said.


ZDNet MENU UK

Hackers are targeting telecom companies to steal 5G secrets

Cybersecurity researchers at McAfee detail an ongoing cyber-espionage campaign that is targeting telecom companies around the world.


REUTERS World Business Markets Breakingviews Video

Hackers hit global telcos in espionage campaign - cyber research firm


NEWS

Home | War in Ukraine | Coronavirus | Climate | UK | World | Business | Politics | Tech

UK | England | N. Ireland | Scotland | Alba | Wales | Cymru | Isle of Man | Guernsey

Briton who knocked Liberia offline with cyber attack jailed


FINANCIAL TIMES myFT

TalkTalk Telecom Group PLC + Add to myFT

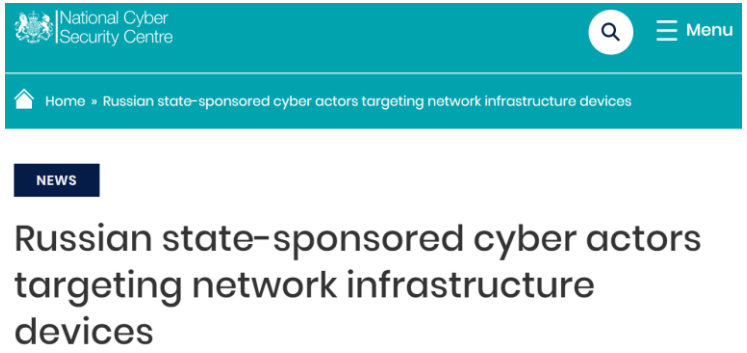
TalkTalk cyber attack: what we know about the hack

Hackers may have used distraction of overloading digital systems before stealing customers' data


News | Opinion | Sport | Culture | Lifestyle

York

UK floods 2015: York suffers phone and internet outages


National Cyber Security Centre Menu

Home » Russian state-sponsored cyber actors targeting network infrastructure devices

NEWS

Russian state-sponsored cyber actors targeting network infrastructure devices


NEWS

Home | War in Ukraine | Coronavirus | Climate | UK | World | Business | Politics | Tech | Science | Health

Technology

Ukraine war: Major internet provider suffers cyber-attack

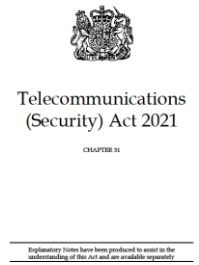

SIGN IN The Register

{* SECURITY *}

UK VoIP telco receives 'colossal ransom demand', reveals REvil cybercrooks suspected of 'organised' DDoS attacks on UK VoIP companies

Background to the Telecoms Security Act

- Ofcom has regulated the security of telecoms since 2011
- DCMS conducted the UK Telecoms Supply Chain Review. Report recommended a new set of security requirements and an enhanced legislative framework.
- The Telecommunications (Security) Act 2021 was passed in November 2021.
- DCMS consulted on its Code of Practice and Regulations. Laid in Parliament on 5 September 2022.
- New regime commenced on 1 October 2022. Supersedes the existing s105A-D in the Communications Act.



The Telecoms Security Act is in two parts

Part 1: Telecoms Security Framework

Strengthened security duties for telecoms providers in legislation and underpinned by statutory guidance in a Code of Practice

Ofcom's role

- General duty of Ofcom to ensure providers' compliance with security duties
- Monitor compliance against legal obligations
- Carry out enforcement action where appropriate
- Provide regular reports to the Secretary of State

Part 2: High Risk Vendors (HRV)

New national security powers for Government to impose controls on the use of HRV equipment and services in UK telecoms networks

Ofcom's limited role

Only when directed by the Secretary of State

- Monitor compliance against legal obligations
- Provide factual reports to the Secretary of State

Roles in this framework

Ofcom

- UK's independent communications regulator.
- General duty to ensure that providers comply with their security duties.
- Clear remit to work with providers to improve their security and monitor compliance.

Department for Digital, Culture, Media and Sport (DCMS)

- Government policy lead for telecoms sector security.
- DCMS Secretary of State may issue regulations and statutory codes of practices.

National Cyber Security Centre (NCSC)

- UK's technical authority for cybersecurity.
- Ofcom and NCSC has published a joint statement on how we will be working in a collaborative, open and transparent manner.

Building blocks of the Telecoms Security Framework

Telecoms Security Framework

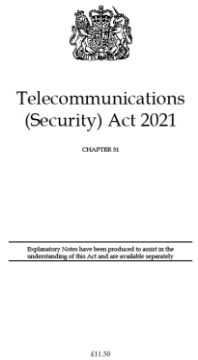
Ofcom's general policy on ensuring compliance with security duties

Royal Assent received Nov '21

Proposals consulted by DCMS and laid in Parliament Sept '22

Policy and guidance consulted by Ofcom

Primary legislation



Telecommunications (Security) Act 2021

CHAPTER 31

Explanatory Notes have been produced to assist in the understanding of this Act and are available separately

£11.50

High-level overarching legal duties

Secondary legislation

STATUTORY INSTRUMENTS

2022 No. 933

ELECTRONIC COMMUNICATIONS

The Electronic Communications (Security Measures) Regulations 2022

CONTENTS

c. 50 specific security requirements

Supplemented by

Draft Code of practice

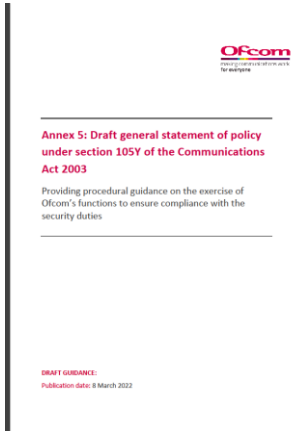
Department for Digital, Culture, Media & Sport

Draft Telecommunications Security Code of Practice

c. 250 guidance measures for complying with legal obligations

Final Code of Practice will be published after Parliamentary scrutiny

Procedural guidance



Ofcom

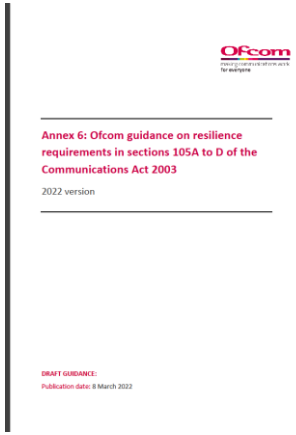
Annex 5: Draft general statement of policy under section 105Y of the Communications Act 2003

Providing procedural guidance on the exercise of Ofcom's functions to ensure compliance with the security duties

DRAFT GUIDANCE:

Publication date: 8 March 2022

Resilience guidance



Ofcom

Annex 6: Ofcom guidance on resilience requirements in sections 105A to D of the Communications Act 2003

2022 version

DRAFT GUIDANCE:

Publication date: 8 March 2022

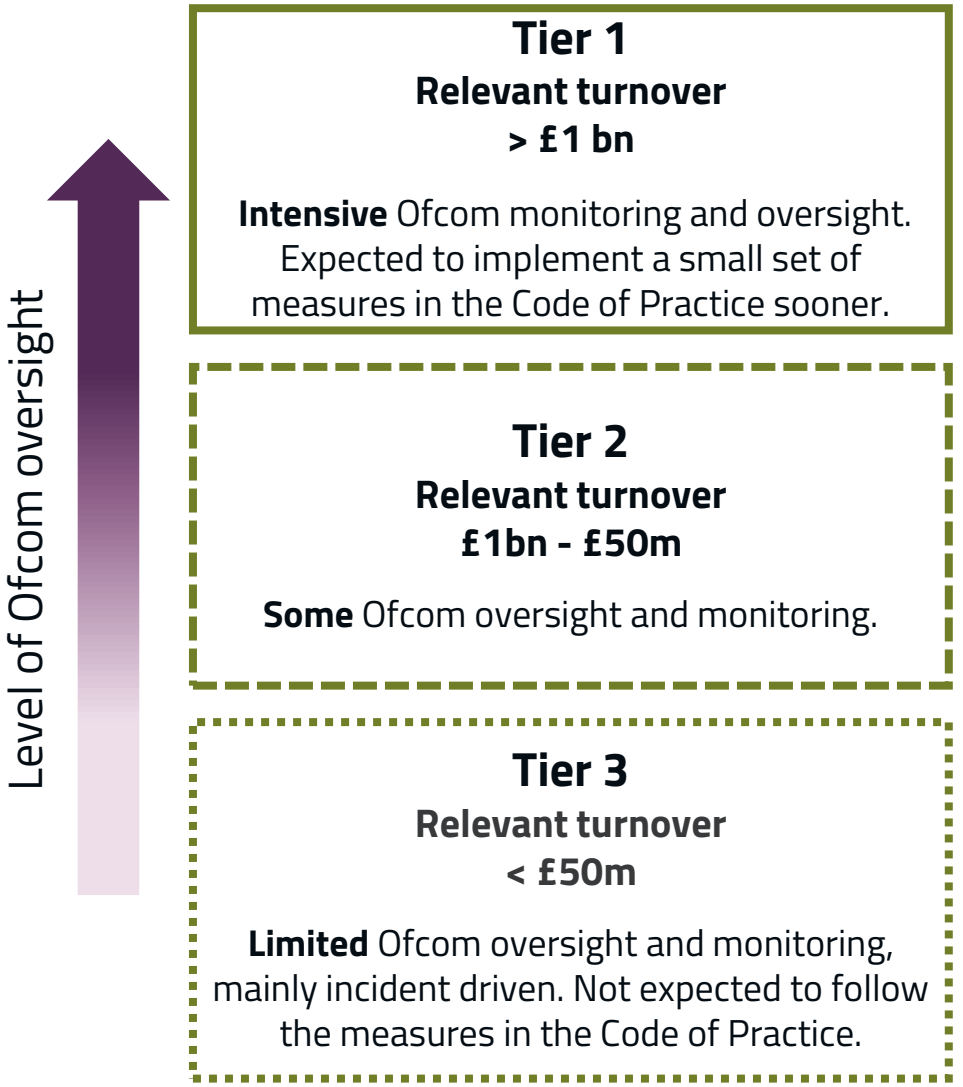
Policies and procedures on how Ofcom will carry out its monitoring and enforcement activities, as well as the incident reporting process for industry

Ofcom's consultation statement and finalised guidance will be published shortly after the final DCMS Code of Practice is published.

Tiering mechanism in the DCMS Code of Practice

The framework applies to all providers of
Public Electronic Communications Networks (PECN)
and **Public Electronic Communications Services (PECS)**

- DCMS has set out three tiers of providers in their Telecoms Security Code of Practice
  - **Tier 1:** largest national-scale providers
  - **Tier 2:** medium-sized providers
  - **Tier 3:** the long-tail of smaller providers
- Revenue-based metric to determine tiering.
- Same 'Relevant Turnover' definition as data already submitted to Ofcom for admin fees charging.
- Level of Ofcom oversight dependent on tiering.



Telecoms Security Code of Practice

- Statutory guidance issue by the DCMS Secretary of State.

- The Code of Practice includes:
  - Details on the tiering mechanism.
  - Key security concepts to aid understanding.
  - c.250 guidance measures mapped to legal duties.
  - Expected implementation timeframes for Tier 1 and 2.

- Providers may deviate from the Code, but must explain to Ofcom how the alternatives still meets the law.

- Currently in draft form:
  Laid in Parliament for scrutiny – 40 sitting days.
  Final Code of Practice expected in December.

Telecoms Security Code of Practice: Key concepts

1. Overarching key concepts
2. Network architecture
3. Protection of data and network functions
4. Protection of certain tools enabling monitoring or analysis
5. Monitoring and analysis
6. Supply chain
7. Prevention of unauthorised access or interference
8. Preparing for remediation and recovery
9. Governance
10. Reviews
11. Patching and updates
12. Competency
13. Testing
14. Assistance

Department for Digital, Culture, Media & Sport

Draft Telecommunications Security Code of Practice

Telecoms Security Code of Practice: Cross-cutting themes

Privileged access workstations

A network can only be as secure as the devices that are able to administer the network

and so implementing a high level of security assurance for administrative devices is essential.

Guidance in the Code of Practice highlights key aspects:

- Non-privileged user accounts
- Feeds into monitoring
- VPNs and remote access
- Cross-domain working
- Known-good operating system images
- Approved application list
- Encryption
- Regular updates
- Approved removable media list

Virtualisation

The use of this technology is growing significantly across the telecoms sector.

Virtualisation can enable for greater flexibility. Operationally it allows services to scale up and down easily.

In terms of network security, additional security controls can be added, interfaces can be monitored,

or processes can be inspected without affecting on-going services.

Virtualisation can be an effective tool for improving the security of a system. By enforcing

Telecoms Security Code of Practice: Cross-cutting themes

Supply chain security

Telecoms providers need to fully understand and reduce supply chain risks.

One of the key aims is to ensure providers flow down security requirements to third-party suppliers by contractual arrangement and ensuring the supplier is working to the same security standards in terms of the goods, services or facilities it supplies to the provider.

The Code of Practice includes the NCSC's Vendor Security Assessmen
which provides advice on how to assess the security of network equip

The VSA covers multiple topics including:

- Product lifecycle and security management
- Protected development/build environments
- Exploit mitigations
- Secure updates and software signing
- Hardware root of trust and secure boot
- Security testing
- Secure management and configuration
- Vulnerability and issue management

Assessing the cyber risk due to a vendor requires:
- Evidence from the vendor themselves
- Testing to validate the vendor's claims
- Third party evidence

Ofcom's procedural guidance and resilience guidance

- Ofcom is required to set out its general policy on ensuring compliance with security duties
- Comprises of two documents:
  - **Procedural Guidance**

    Procedures we expect to follow in our monitoring and enforcement activities.

    New guidance on which security compromises we would expect providers to report to us.

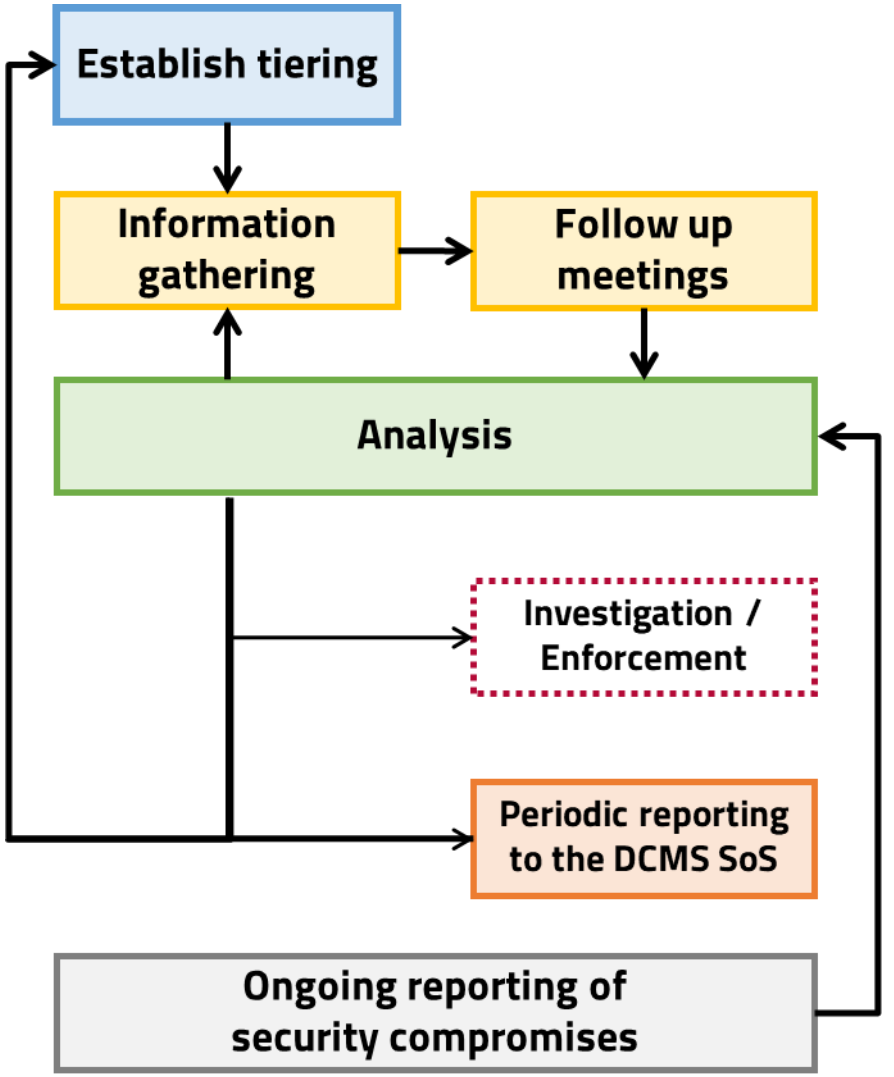
  - **Resilience Guidance**

    Update our existing guidance on network resilience to reflect the new framework.

- Consultation closed – we are currently considering responses.
- Aim to publish our guidance shortly after the finalised DCMS Code of Practice is issued.

Ofcom's proposed approach to compliance monitoring

- **Establish tiering**
  Using thresholds in DCMS Code of Practice.
- **Information gathering**
  To collect the information need for Ofcom to assess compliance.
- **Analysis**
  Determine whether there are potential concerns.
- **Follow up meetings**
  Where we have questions, concerns, or need further information.
- **Formal investigation**
  Consider enforcement in the event of non-compliance.
- **Reporting to Secretary of State**
  Ofcom will submit reports on the extent of industry compliance.
- **Ongoing reporting of security compromise**
  All providers are required to report. Ofcom will investigate if needed.



* Based on the proposals in the Ofcom consultation on its general policy on ensuring compliance with security duties

Ofcom's information gathering powers

- Our objectives at the start of the regime:
  - Build our understanding of providers' networks and services
  - Determine if measures are implemented at sufficient pace
- Ofcom has broad information gathering powers under the Act.
- Our process will primarily be based on s135 information notices.
  - Well established statutory process requiring evidence to be submitted.
- We have a range of other powers which we can use if necessary
  - Interview people involved in network provisioning
  - Enter business premises to observe relevant operations or to gather relevant documents and information
  - Mandate security assessments and testing

Info gathering programme **Indicative timeline***		
	Tier 1	**Tier 2**
1. Establish which tier a provider falls under	Up to 3 months	
2. Initial s.135 info notice: Scoping networks, services and assets	4 months	6 months
3. Subsequent information gathering process		
S.135 info notice frequency:	Approx. every 6 months	Approx. every 9 months
Time allowed for providers to respond:	4 months	6 months

* Based on the proposals in the Ofcom consultation on its general policy on ensuring compliance with security duties

Ofcom's enforcement powers

- Ofcom's investigation can be triggered from different sources
  - Notification of a security compromise
  - Routine Ofcom monitoring
  - Third-party complaints
- The Telecoms Security Act introduces tougher penalties significantly higher than the previous maximum of £2 million.
- We will seek to hold constructive discussions with providers to ensure they take appropriate steps towards compliance.
- However we stand ready to take enforcement as needed.

Ofcom's enforcement powers in the Act

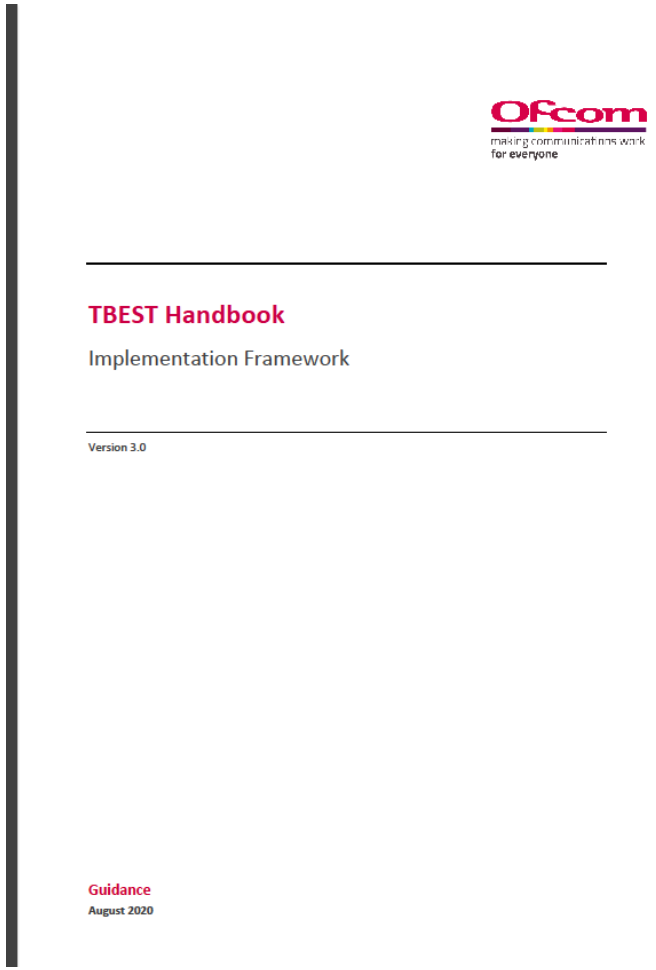
Issue penalties
up to 10% of relevant turnover
Previously £2m max

Issue penalties
up to £10m for failure to provide required information

Instruct providers to take **'interim' steps** to address a security compromise

Testing

- Providers are required by law to carry out regular testing to assess the risk of security compromises.
- Ofcom has the power to carry out or commission specific testing.
- This includes pen-testing and red-teaming exercises.
- Ofcom's voluntary pen-testing programme (TBEST) will continue.
- A provider who undergoes TEBST is showing security maturity and it will help provide real-life improvements in security.
- Testing can provide valuable insight on weaknesses and vulnerabilities to the participant.



Reporting security compromises

- All providers are required to report security compromises to Ofcom.

105K Duty to inform OFCOM of security compromise

(1) The provider of a public electronic communications network or a public electronic communications service
must inform OFCOM as soon as reasonably practicable of -

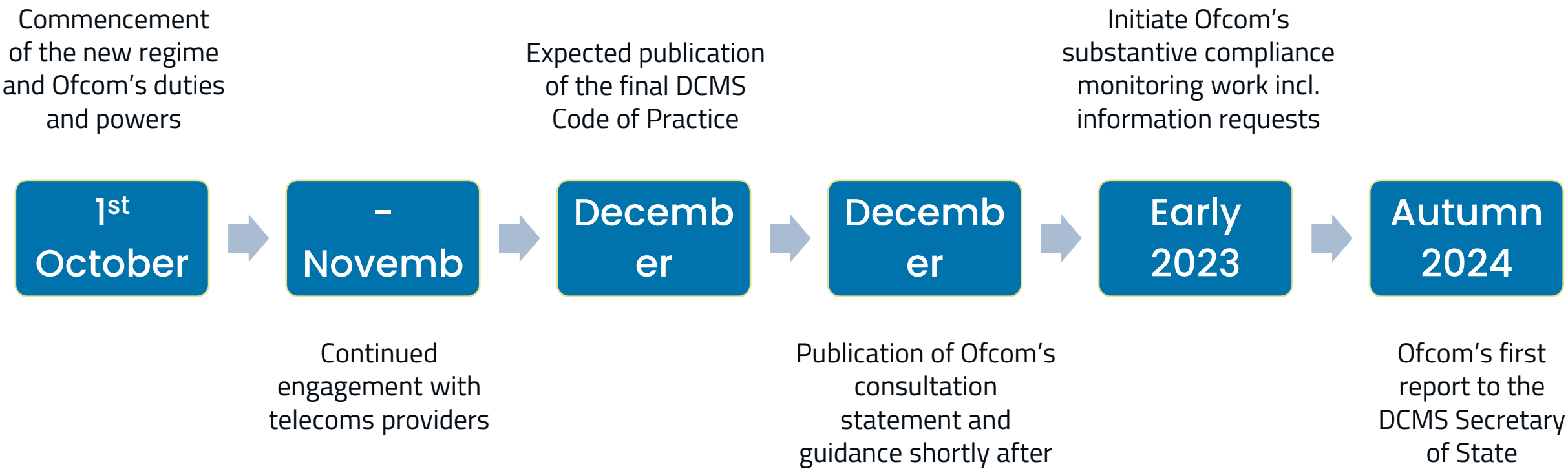
(a) any security compromise that has a significant effect on the operation of the network or service;

(b) any security compromise within section 105A(2)(b) that puts any person in a position to be able to bring
about a further security compromise that would have a significant effect on the operation of the network or service.

- Ofcom has consulted on its general policy on ensuring compliance with security duties.

- Providers are expected to adjust internal processes to meet our new guidance within a reasonable period following the publication of our final statement.

Timeline


Commencement of the new regime and Ofcom's duties and powers
1st October
-
Novemb
Continued engagement with telecoms providers
Expected publication of the final DCMS Code of Practice
Decemb er
Publication of Ofcom's consultation statement and guidance shortly after
Decemb er
Initiate Ofcom's substantive compliance monitoring work incl. information requests
Early 2023
Autumn 2024
Ofcom's first report to the DCMS Secretary of State

Join the team!

- We continue to build our capability and strengthening our skills in cyber security.

- We are actively recruiting specialists to join our team in London and the new tech hub in Manchester.

- See our vacancies here: https://www.ofcom.org.uk/about-ofcom/jobs