Classification: CONFIDENTIAL

Ofcom

Network and Services Resilience Guidance

Nov 2024

Classification: CONFIDENTIAL

Agenda

Overview of Ofcom’s Resilience Guidance

Mobile Power Resilience

1 June 2023

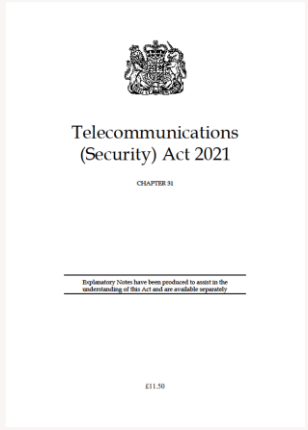
Telecoms Security and Resilience Legal Framework

-> recap on how 'resilience' fits in

Telecoms Security Framework

Ofcom's general policy on ensuring compliance with security duties (including 'resilience')

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

Telecommunications (Security) Act 2021
Section 105 of CA2003

Overarching security duties (inc resilience) and incident reporting obligations

Secondary legislation

STATUTORY INSTRUMENTS

2022 No. 933

ELECTRONIC COMMUNICATIONS

The Electronic Communications (Security Measures) Regulations 2022

CONTENTS

Electronic Communications (Security Measures) Regulations 2022

Duties to take specific security measures

Supplemented by

Statutory guidance

Department for Digital, Culture, Media & Sport

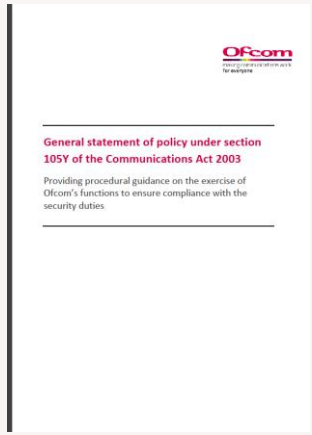
Telecommunications Security Code of Practice

December 2022

Telecommunications Security Code of Practice

Cyber security focused guidance measures for complying with legal obligations

Procedural guidance



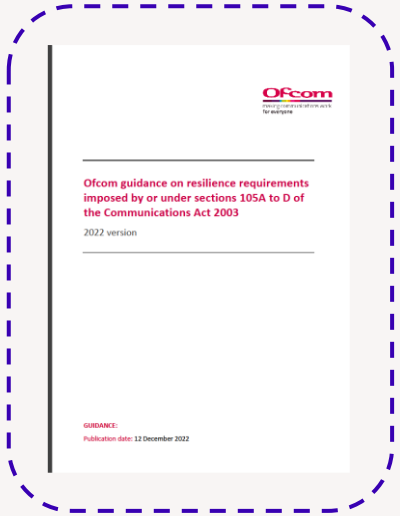
Ofcom

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

Procedural Guidance
How Ofcom will carry out its monitoring and enforcement activities, & incident reporting process for industry

CP Resilience guidance



Ofcom

Ofcom guidance on resilience requirements imposed by or under sections 105A to D of the Communications Act 2003

2022 version

GUIDANCE:

Publication date: 12 December 2022

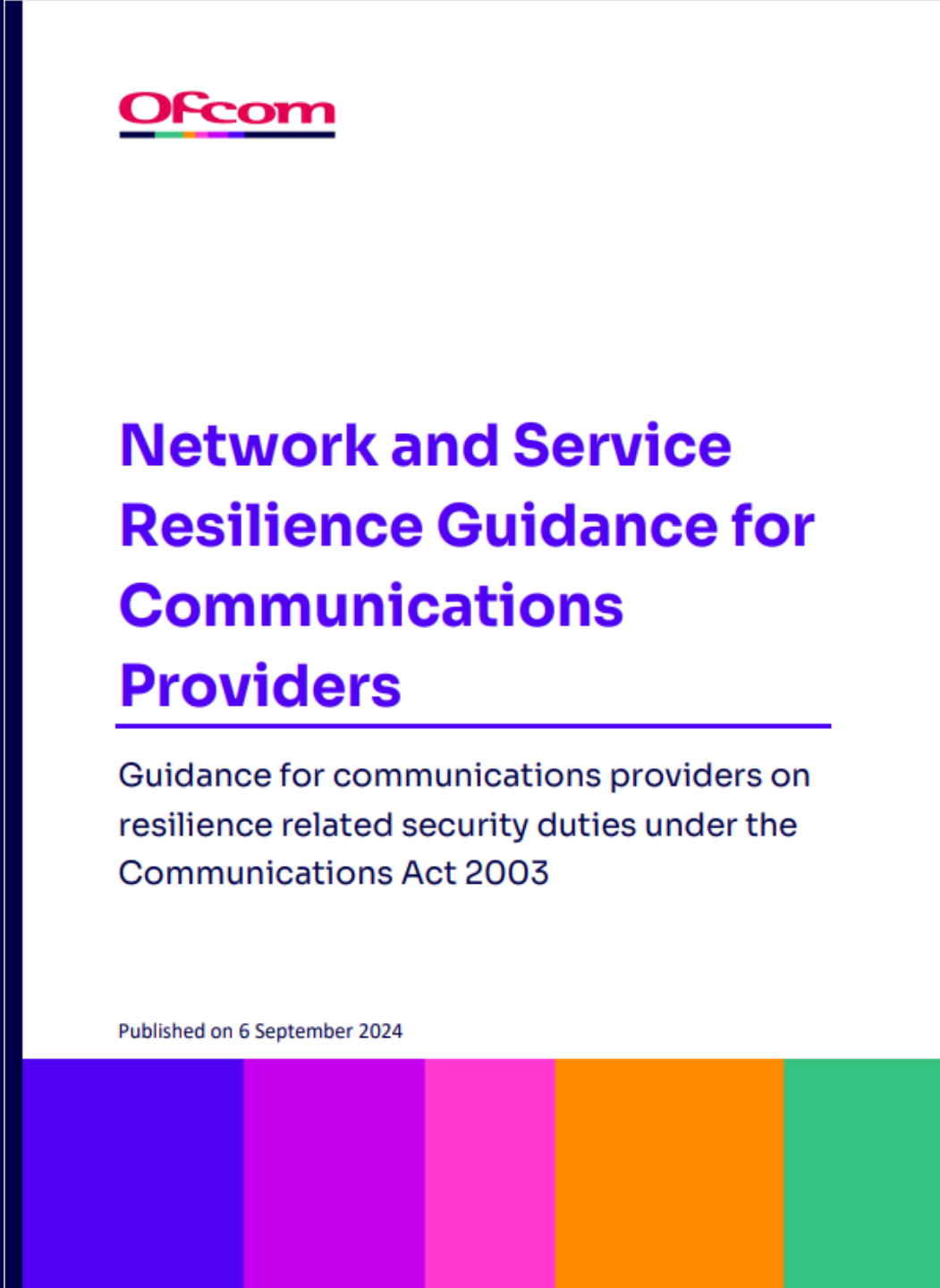
Network & Service Resilience Guidance for Communications Providers

'Resilience' focused guidance measures for complying with legal obligations

Ofcom's Resilience Guidance

Significant update of our 2022 guidance to provide greater clarity on how UK telecoms companies can reduce the risk of network outages.

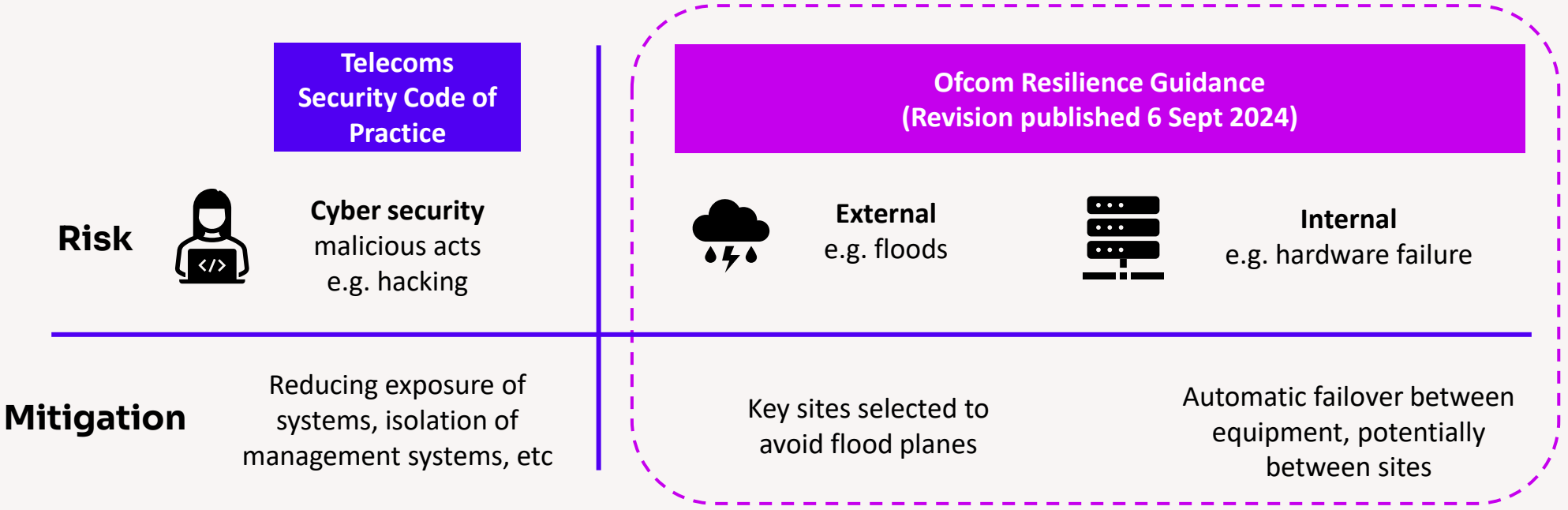
Updated version published on 6 Sept 2024



Telecoms Network Resilience

- Telecoms providers must take appropriate and proportionate measures regarding:
  - identifying and reducing the risks of security compromises *(including resilience incidents)* occurring
  - preparing for the occurrence of security compromises *(including resilience incidents)*

- Ofcom's resilience guidance sets out **technical measures** we expect operators to take in relation to the **resilience of their networks and services.**



Resilience Guidance contents

Our guidance describes **a range of practices in the architecture, design, and operational models** that underpin robust and resilient telecoms networks and services, as well as more specific measures that we expect providers to consider.

This includes:

- Ensuring that networks are designed to avoid or **reduce single points of failure**;
- ensuring that key infrastructure points have **automatic failover** functionality built in.
- setting out the **processes, tools, and training** that should be considered to support the requirements on resilience.
- **Enhancing reliability** for **critical services**

Areas of resilience	
Access/Last Mile	Network Infrastructure Domains
Aggregation/Backhaul	
Core	
Peering and Interconnect	
Power backup in access, aggregation, and core networks	
Control Plane	Logical Planes and Services
Management Plane	
Enhancing reliability for critical services (eg voice)	
Network and service design and planning criteria	Process, tools, and training
Network and service testing, deployment, change control	
Network/Service operation, monitoring, and processes	
Skills competency training	

Classification: CONFIDENTIAL

Power Resilience in Access Networks

Why is Ofcom exploring mobile power resilience?

As we increasingly rely on mobile services to stay connected, it is becoming more important that mobile networks are resilient.

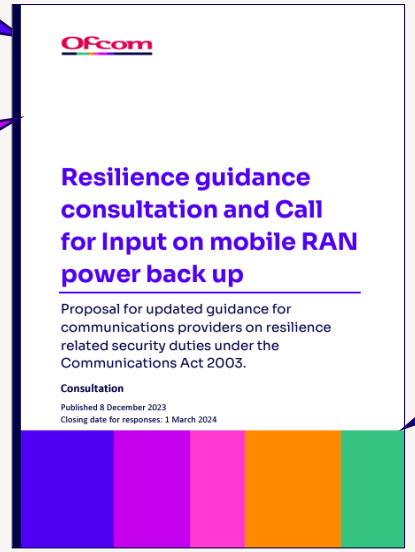
A key risk to mobile networks is the availability of UK mains electrical power. There is some degree of existing electrical power backup within the mobile access networks, but the number of sites and duration of the back-up varies.

Our Call For Inputs (CFI) explores what additional measures MNOs could take regarding the extent of power backup at mobile RAN sites

'The single most effective step to improve the reliability of the UK's mobile and fixed communication networks is to better assure the power grid, making it more robust and better able to withstand weather events, while simultaneously improving processes to prioritise mobile sites for restoration should power be lost.' **Vodafone response.**

We think Ofcom, as an expert adviser to Government, is well-positioned to consider – for example – how electronic communications networks could be more promptly reconnected to mains power, or what tools might be made available from energy networks to assist in mobile network planning. **BT/EE Response**

CFI responses highlighted crucial role of the energy sector



'In a hierarchy of CNI on which all others depend, electricity supply is at the apex. The regulations imposed on the energy supply industry should reflect this, as it clearly should play a vital role in strengthening the energy resilience of all the sectors it serves. **VM02 Response**

Ofcom's work and what next?

Levels of alternative backup power (batteries or generators) **varies across the 4 UK MNOs**. Ranges from 5 days to 15 mins to nothing

Upgrades would be **costly** - 1 hour for all sites = £0.9-1.8bn.

International approaches:

Switzerland	72hrs at some sites	Proposed legislation
Australia	12 hrs at sites affected by bush fires	Direct Govt funding
Norway + Finland	2-6hrs	Strong regulation

Resilience of power networks is the responsibility of energy sector.
But availability of services in sectors that depend on the energy networks is a **cross-industry and Government challenge.**

Ofcom's work

- We have put industry best practice into guidance where it is already consistent: Core – 5 days backup, fixed cabinet – 3-4hrs.
- Responses from our CFI suggested targeting more 'at risk' sites of a power outage with backup.
- Our next step is to model voice coverage during power cuts, to understand vulnerable areas and model costs to address this, to share with Government.
- We're working with the energy industry. Improving co-ordination during incidents, and information on restoration allows telcos to prioritise, e.g. tow to site generators

Classification: CONFIDENTIAL

Thank You

Classification: CONFIDENTIAL

Contact

Gina Baikenycz
Principal Technology Advisor
gina.baikenycz@ofcom.org.uk

www.ofcom.org.uk