



## 1.0

# Why is this document relevant?

Telecommunication networks are the backbone of digitalisation, underpinning many essential services and sectors through trusted and secure communication systems which impact society as a whole. For this reason, ongoing security and integrity must be at the forefront of telecommunication preparedness. This includes planning for the quantum era and the potential threats that quantum computers pose to telecommunications networks, customer data and devices.

---

This document provides detailed insights for preparing a cryptographic migration and implementation of post quantum cryptographic capabilities in the context of telecommunication networks, analysing use cases and architecture, highlighting dependencies on standardisation, solution alignment, performance testing and related topics such as Zero Trust Architecture.

The objective is to build a set of best practice guidelines to support an executable journey to quantum safe for operators and the wider telecommunication ecosystem, leveraging learnings and evolving a collective view of solutions and standards that support interoperability, backward compatibility and performance requirements.



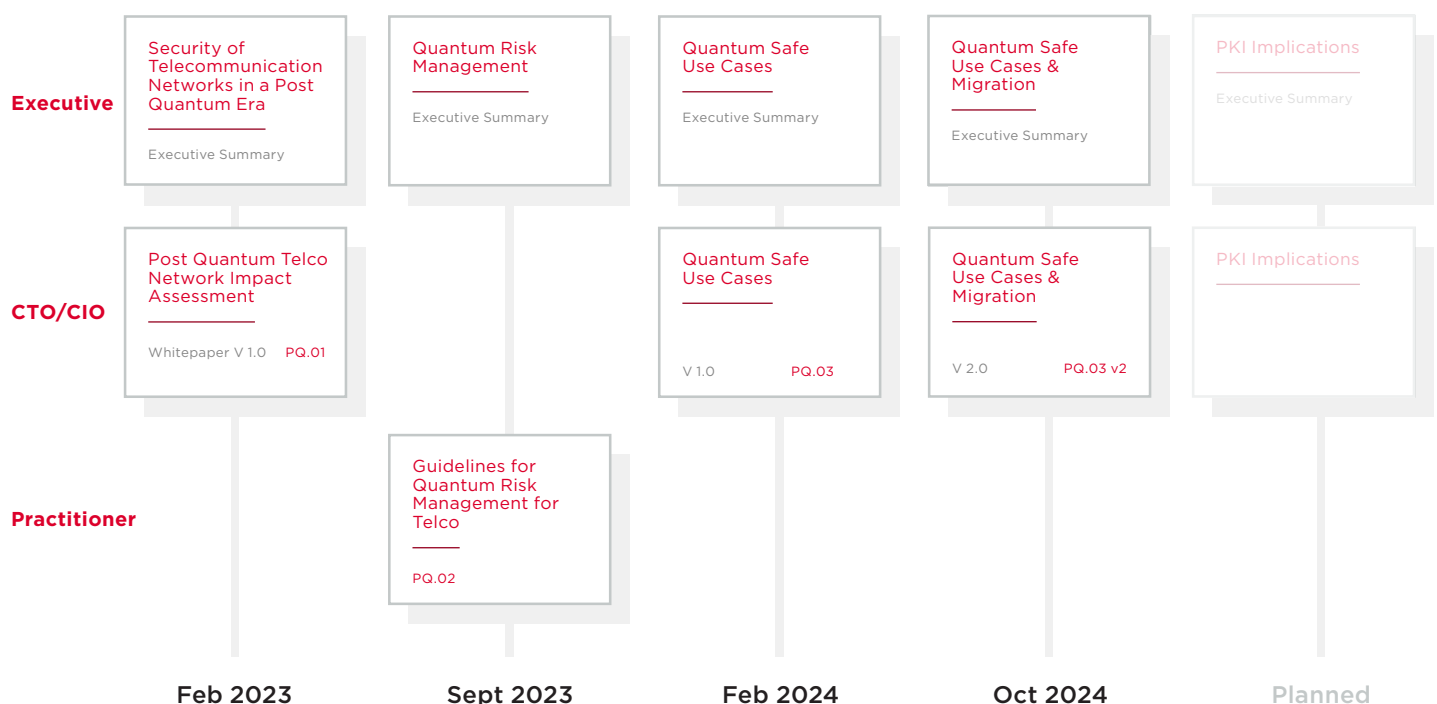
## 2.0

## How do we see It evolving?

This is the second version of a working document that covers an initial set of telco use cases impacted by post quantum cryptography. Over time we plan to update and add to these use cases as required, and explore the relevant technology, standards or policies to inform telco ecosystem decision makers.

This will provide a telco-focused, practical and actionable perspective, based on learnings, experience and best practice. The relationship between this document and previous PQTN task force publications is illustrated in Figure 1. In the second revision the timelines and dependencies paragraph has been updated, an algorithm and protocol standards status update has been

provided based on the progress since the last revision, Including the standardisation of the first NIST PQC algorithms, announced In August 2024. Focus has been on migration strategy considerations: common dependencies and technical features that apply across use cases as well as use case specific migration approaches.

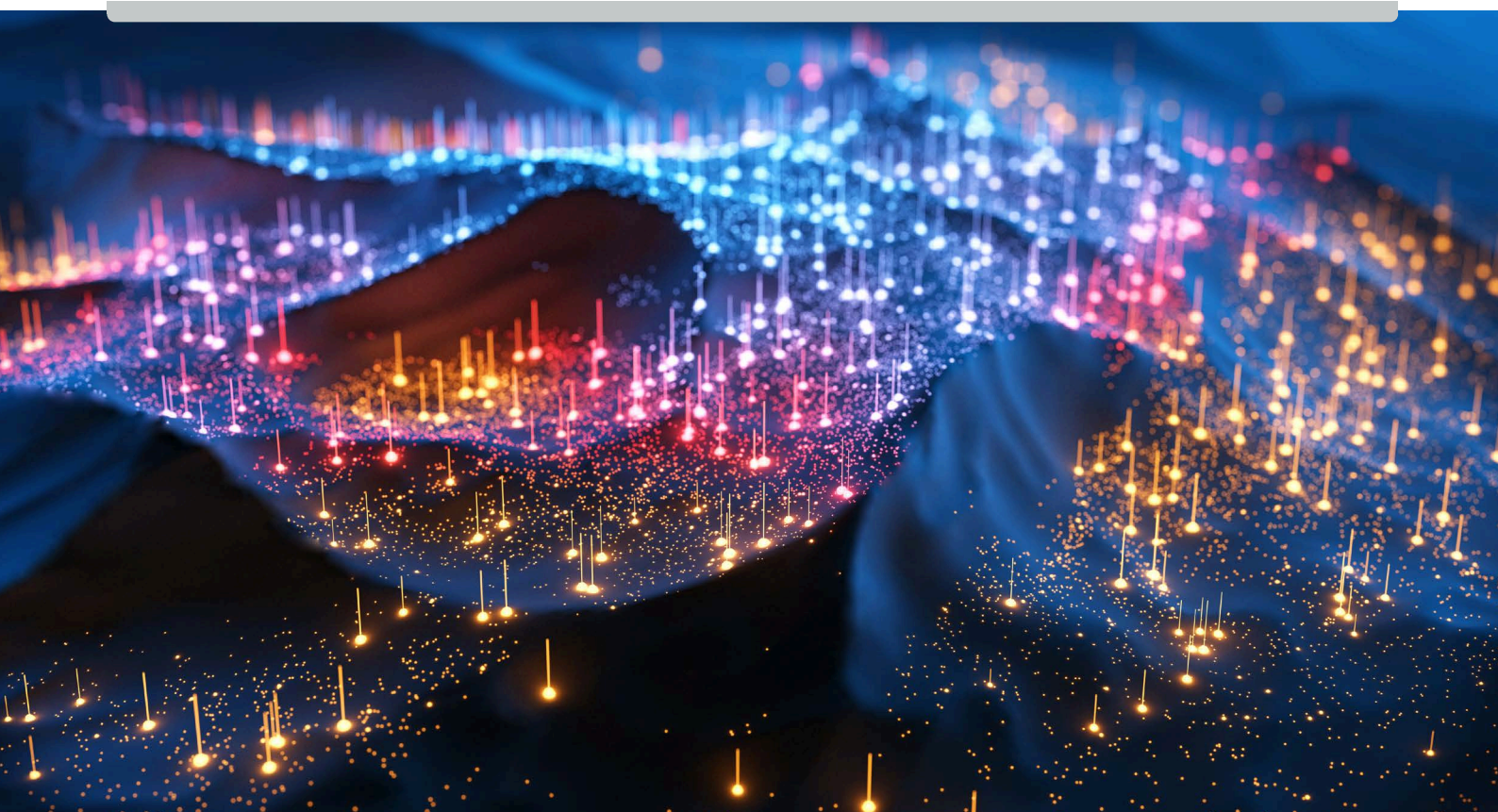
**Figure 1****Taxonomy of PQTN task force publications**



Feedback from the wider ecosystem is essential for the continued relevance of the document. Recognising that many aspects regarding standards, policy and solutions are evolving in parallel and have multiple dependencies, the GSMA PQTN Task Force welcomes the opportunity to engage and foster cooperation between all relevant stakeholders.

Alignment around technology decisions is likely to become critical in the context of interoperability, backward compatibility, and performance.

Developing proofs of concept and testing are essential for timely deployability of commercial solutions.



## 3.0

# What is the Quantum Threat?

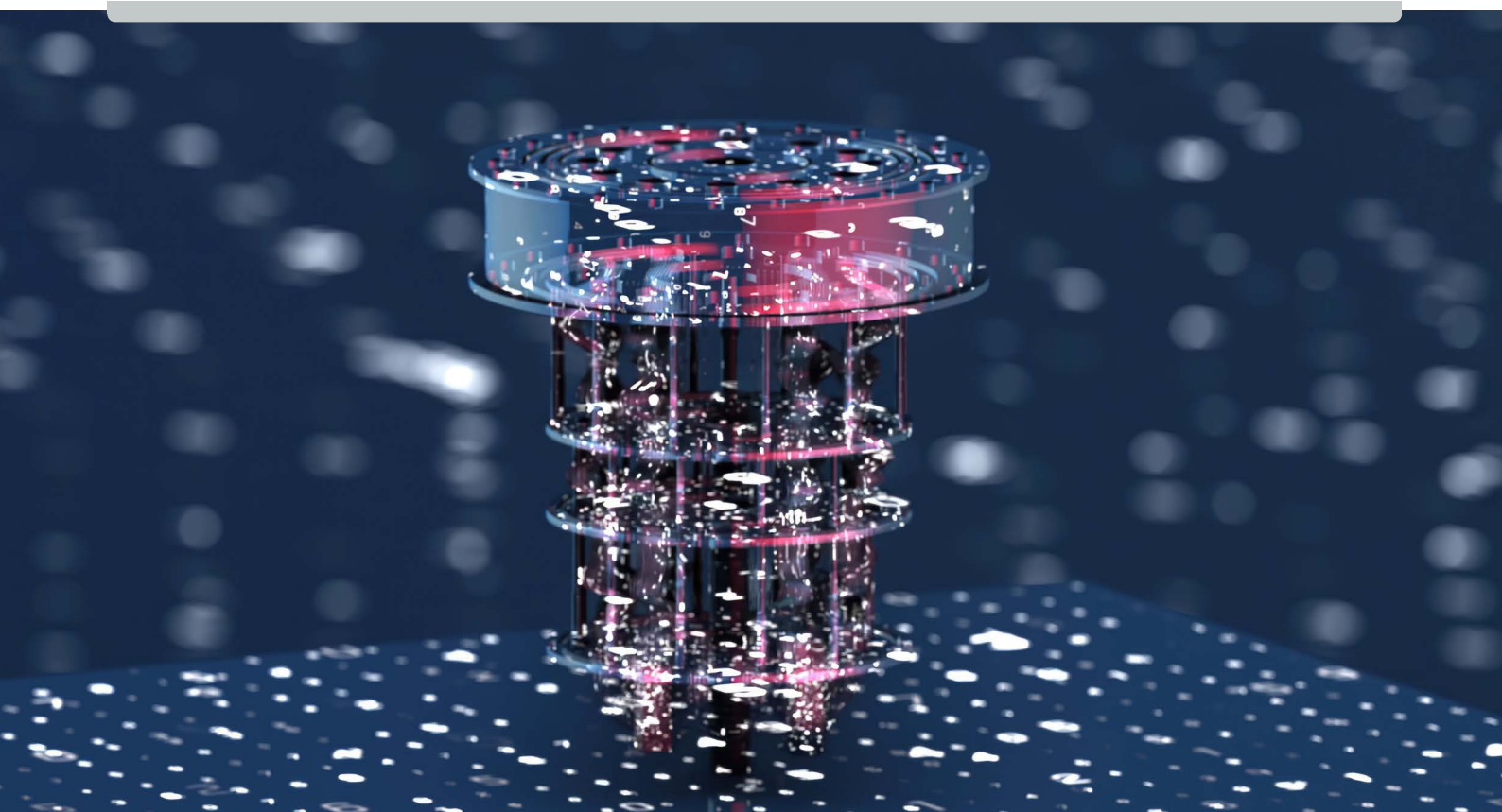
The evolution of quantum computing capabilities poses a threat as they have the potential to render obsolete the most used cryptographic algorithms, such as public key cryptography, which underpin the cyber security solutions we rely on today to keep information and communications safe.

---

The timing of the threat is uncertain, however significant progress is being made in the evolution of quantum computing performance, quantum algorithms, and error correction.

This is particularly relevant for data that has a long shelf life when considering the possible availability of cryptographically relevant quantum computers in the coming years.

The telco industry should start now to plan for the post quantum migration. An immediate threat to consider is “Store now decrypt later”, where encrypted data is harvested in anticipation of being decrypted in the future.



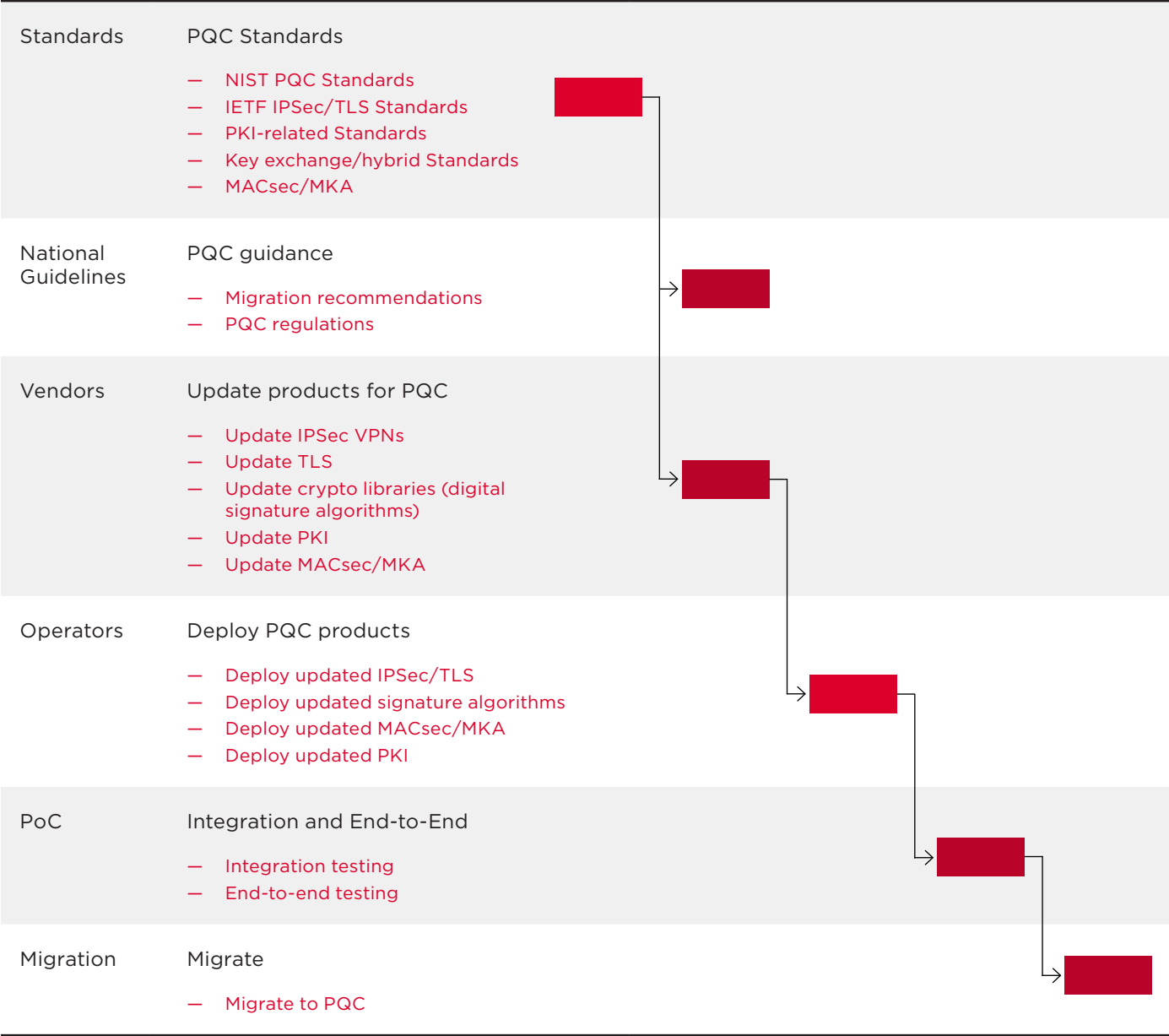
## 4.0

## Use cases, risk analysis and business Impact

For the use cases listed in the table below, an analysis has been provided to inform both business risks and subsequent technology choices, with the addition of information designed to inform a migration strategy such as Gantt Charts, analysis of migration options and dependencies.

| NETWORK OPERATOR USE CASES                                       | CUSTOMER IMPACTING USE CASES     |
|--|----------------------------------|
| Protection of interface between base stations & security gateway | Virtual Private Network services |
| Virtualized network functions                                    | SD-WAN services                  |
| Cloud Infrastructure   | IoT Smart Meters                 |
| SIM (physical)   | IoT Automotive                   |
| eSIM Provisioning (remote)                                       | Lawful Intercept                 |
| Devices and firmware upgrade                                     | Privacy of customer data         |
| Concealment of the Subscriber Public Identifier                  | Enterprise Data                  |
| Authentication and transport security in 4G and 5G               |                                  |
| Network Function Authorization                                   |                                  |

Figure 2  
Gantt chart for VPN PQC migration



## 5.0

## Importance of planning and preparation

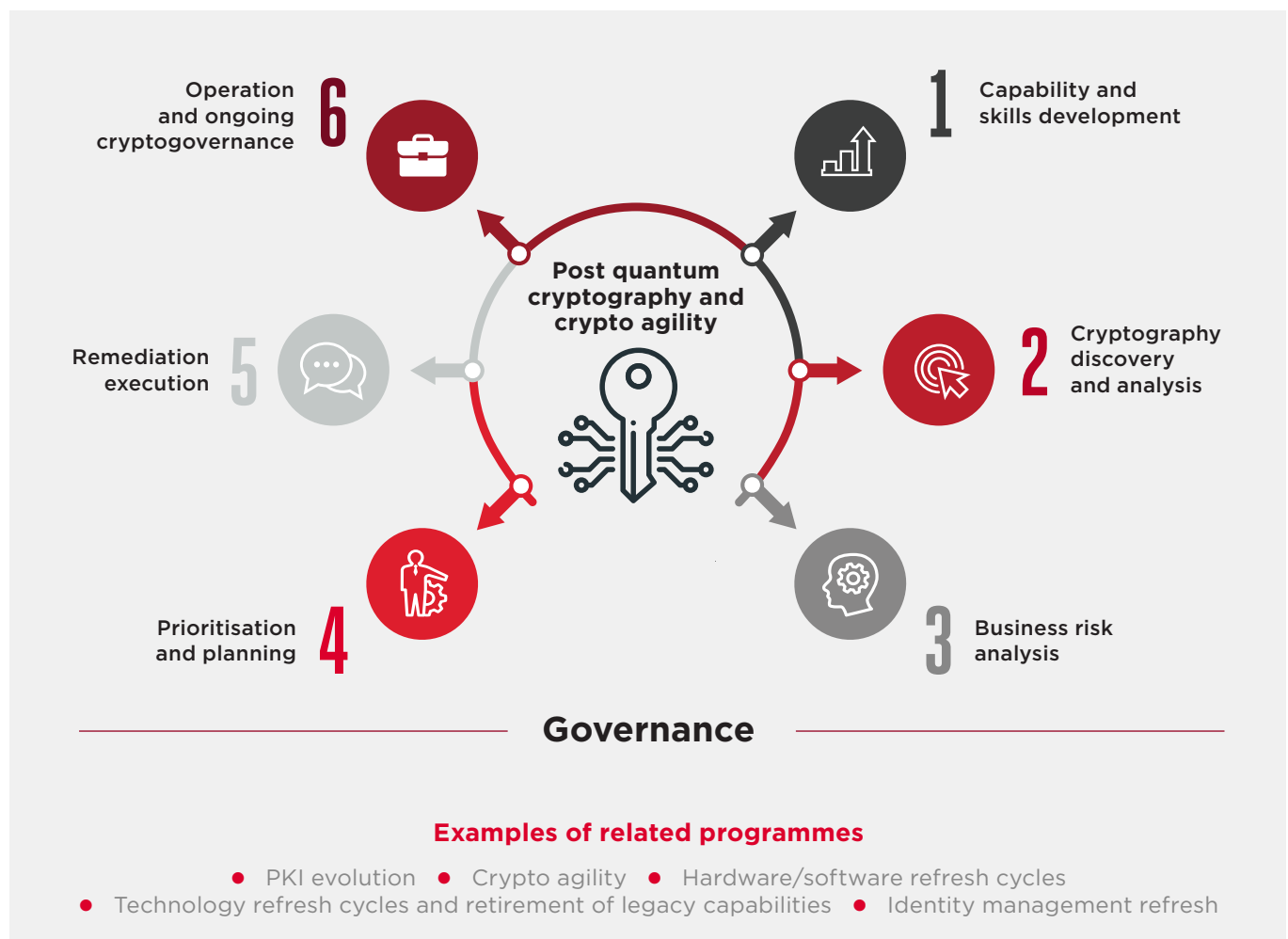
The document provides practical guidelines on how organisations can start to plan, engage with internal and external stakeholders, quantify risk and take action.

Forward planning will provide significant benefits to organisations in managing risks and optimising costs of the post quantum migration. A definition of high-level phases to support

the journey to Post Quantum Cryptography and subsequent management is outlined in Figure 2, illustrating the iterative nature of the phases and the importance of governance.

Figure 3

### A phased journey towards Quantum safe





## Supporting Companies:

---

3 United Kingdom  
AKAYLA  
Arqit  
AT&T Mobility  
Cellular South Inc. d.b.a. C Spire  
China Telecom  
China Unicom  
CK Hutchison  
Deutsche Telekom AG  
EE Limited  
Ericsson  
F5, Inc.  
Fortinet  
Giesecke+Devrient Mobile Security  
Hewlett Packard Enterprise  
Huawei  
IBM  
IDEMIA  
IMDA  
Infineon Technologies AG  
Infobip Ltd  
Juniper Networks  
Kigen  
KT Corporation  
Maxis Broadband Sdn. Bhd.  
National Cyber Security Centre  
Nokia  
NXP

OFCOM  
Orange  
Orange France  
Palo Alto Networks Inc.  
PQ Shield  
Proximus Belgium  
Qualcomm  
Samsung Electronics Co Ltd  
SandboxAQ  
SK Telecom Co., Ltd.  
stc Group  
STMicroelectronics  
Telcel  
Telefonica  
TELUS Communications Inc.  
Thales  
The MITRE Corporation  
TIM  
Turkcell  
Utimaco  
Verizon  
Vodacom  
Vodafone Group

**GSMA Head Office**

1 Angel Lane  
London  
EC4R 3AB  
United Kingdom  
Tel: +44 (0)20 7356 0600  
Fax: +44 (0)20 7356 0601

