



Government and industry reactions to quantum risk in the US

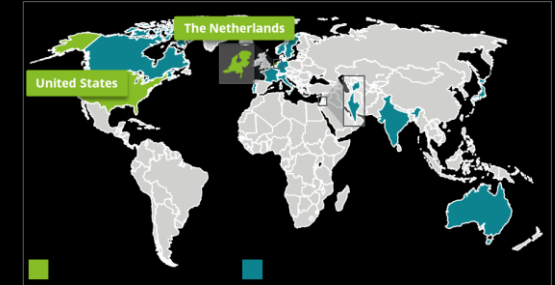
Itan Barmes, Deloitte NL

PQC Symposium, 3 December 2024

Our journey into Quantum Cyber Readiness

Since 2020, Deloitte has been focusing on shedding light on the threat that Quantum Computers pose to cybersecurity. Today, a global team is joining forces to help our clients with their Quantum Cyber Readiness activities

Perspective
Quantum computers and the Bitcoin blockchain
An analysis of the impact quantum computers might have on the Bitcoin blockchain



2020

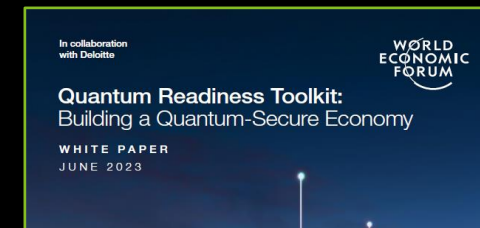
2021

2022

2023

2024

Perspective
Quantum risk to the Ethereum blockchain - a bump in the road or a brick wall?
A quantitative analysis of the quantum threat to the Ethereum blockchain and the transition to a quantum-safe solution



Context & Objectives

The US government has set the transition to PQC in motion. We will discuss how that is impacting the US market in both government agencies and the commercial sector



Outline what US government is doing to promote the adoption of quantum-safe technologies.

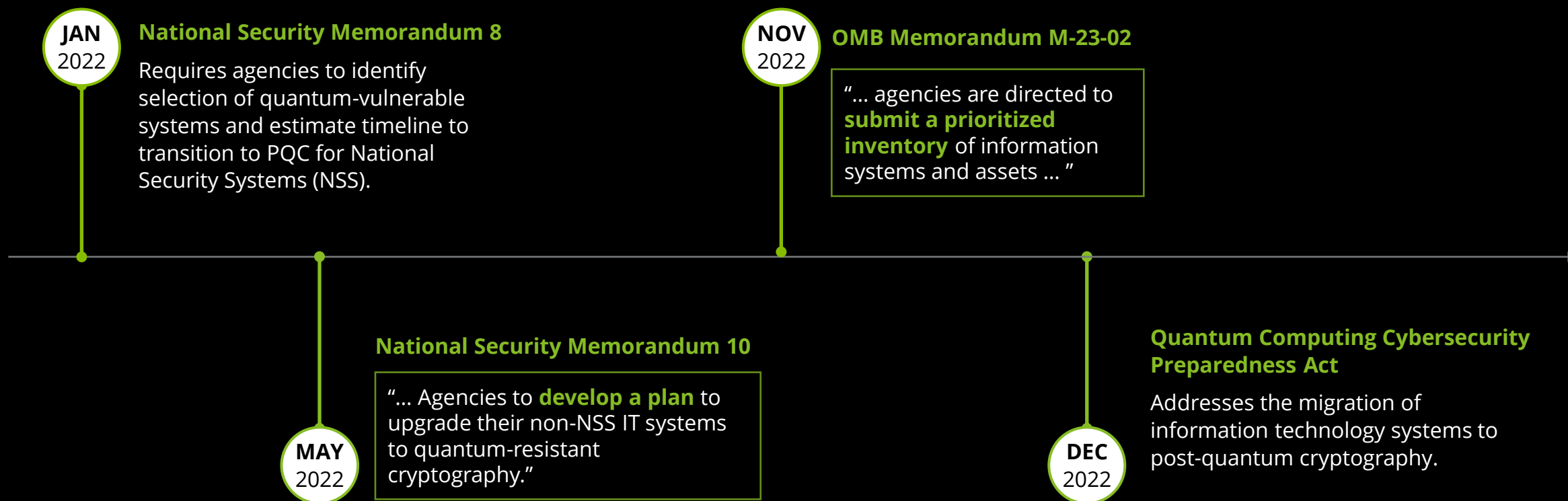


Understand how organizations in the US take action on Quantum security.



The United States' response to cryptographic threats

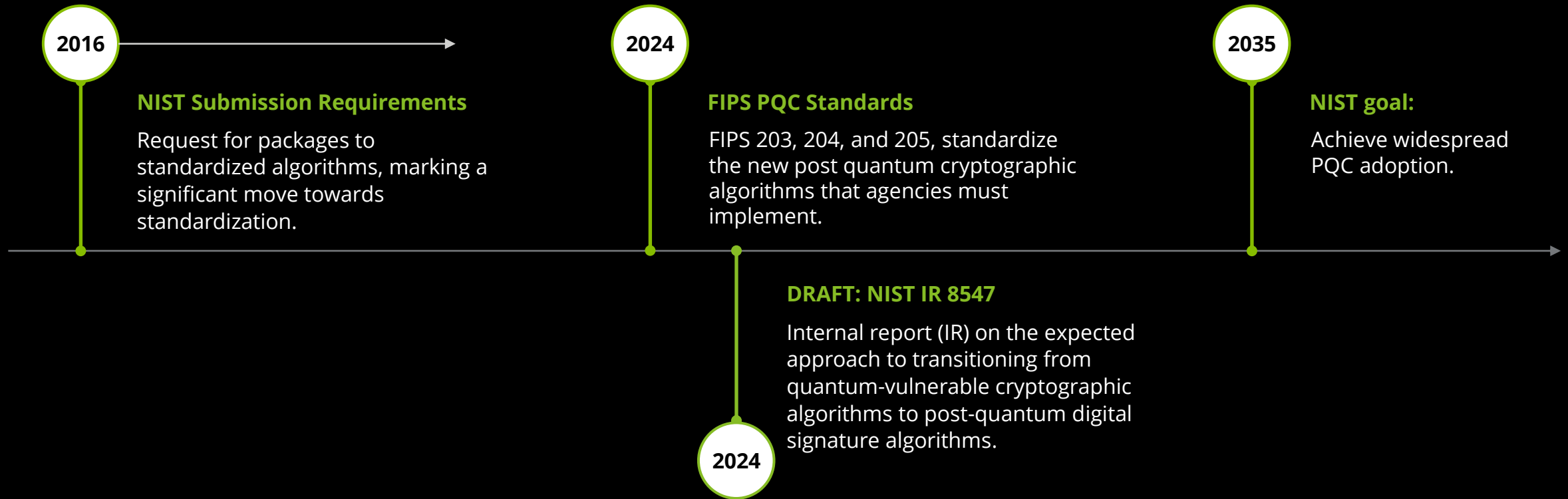
A flurry of executive guidance in the last few years has shown that the U.S. see this as a strategic risk – and that agencies and industry should prepare



Government agencies have also issued guidance on PQC transitions: NCCoE, CISA, NIST, NSA

FIPS are here, so now what?

NIST has been leading the way to standardizing post quantum cryptographic algorithms since 2016, with the objective to reach widespread adoption of PQC by 2035

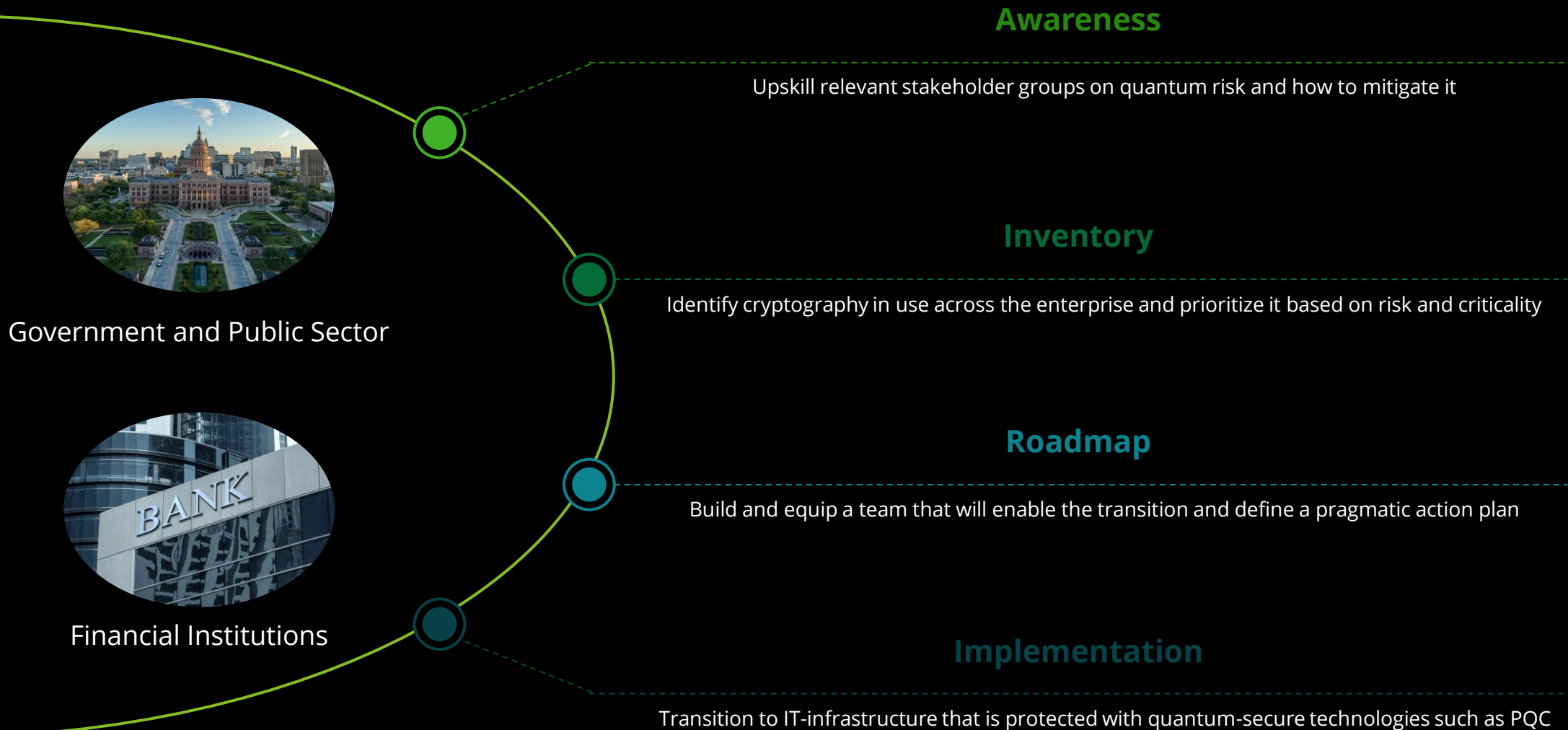


Is this just a (simple) technology upgrade?



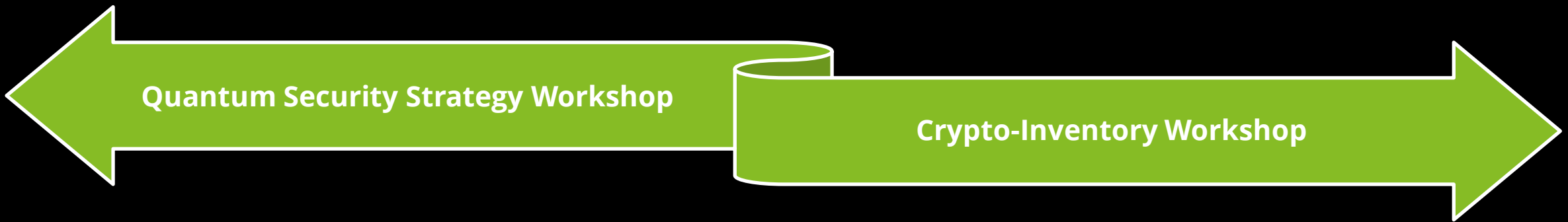
What we see at clients

We see pockets of clear activity on quantum risk and a trend towards more action, with agencies maturing their perspectives and action on quantum readiness



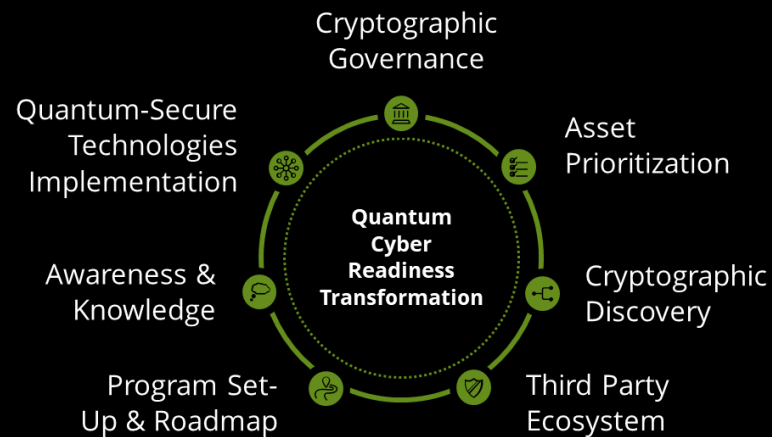
Our work has led us here!

We used our previous experience with clients to build methodologies to mitigate the quantum risk. We see the highest demand in establishing a roadmap, and building a cryptographic inventory



Understand the core domains for your transformation, actions to take and how to prioritize them.

Kickstart your Cryptographic discovery following our demonstrated methodology.



The PQC journey has begun, now where do we go?

The migration to PQC is underway and the journey is not linear. Understanding what has happened and what is forthcoming is critical to accelerating the transition further



The U.S. Government has released **policy to propel PQC** that may have downstream impacts on commercial entities.



We see **meaningful steps** happening in both **Government agencies** and in the **private sector**.



Despite progress, there are still **obstacles** that may slow the PQC transitions. It is paramount to **increase the maturity** how organizations to take the right steps.

This topic requires a steep learning curve – let's learn from each other to grow stronger collectively.

Thank you.

Itan Barmes

Global Quantum Cyber Readiness Capability Lead



ibarmes@deloitte.nl

globalquantumcyberreadiness@deloitte.com

