Bloor

# InBrief

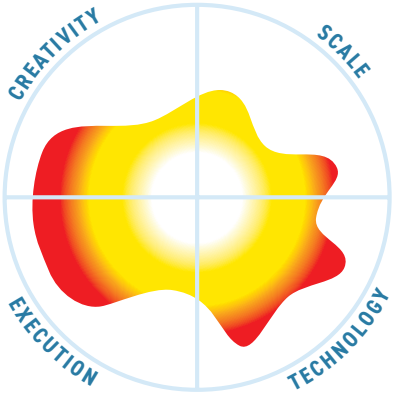
**Alan Rodger** – Senior Analyst, Security and Cloud

# Quantum Cyber GRC, by Cystel

**www.cystel.org**

Clavering House, Clavering Place, Newcastle Upon Tyne, NE1 3NG, England
Tel: +44 333 1223 372 Email: info@cystel.org

This **Mutable Quadrant** is derived from 13 high level metrics, the more the image covers a section the better. **Execution** metrics relate to the company, **Technology** to the product, **Creativity** to both technical and business innovation and **Scale** covers the potential business and market impact.




## The company

Cystel is a British cybersecurity company that specialises in a scientific approach to the next generation of protection problems that will face security leaders. It has differentiating capabilities that can help its customers address the upcoming major problem of next-level threats arising in the quantum computing age.

In general terms, Cystel offers services and solutions covering requirements that aren't widely addressed by mainstream cybersecurity markets. These include hacker profiling, security architecture/policies assessment, security operations centre (SOC) functions including threat management and incident response capabilities, and the delivery of a security awareness program – as well as Quantum Cyber GRC training, which is the main topic of this paper. (GRC is the abbreviation of 'governance, risk, and compliance').

The company was founded in 2018 by Dr. Meera Sarma (now CEO), with Dr. Thomas Matheus (now CTO), and Rishi Tarar (now CIO) as co-founders. It has focused on industry sectors that are typically most targeted by hackers and other threats i.e. banking and financial services, healthcare, critical infrastructure, energy, smart cities, and telecoms. It has a partnership with PwC, and has the status of a Crown Commercial Service Supplier in the UK. Its engagements until now have been in the UK and LATAM, and it will launch in the MENA region in 2H24.

## What is it?

Quantum computing (QC) has been under development for decades, but according to all informed industry predictions, it will become widely used in just a few years. Its exponentially greater computing power/speed, and a fundamental difference in logic foundation, will offer many transformational opportunities. However, it has long been understood that

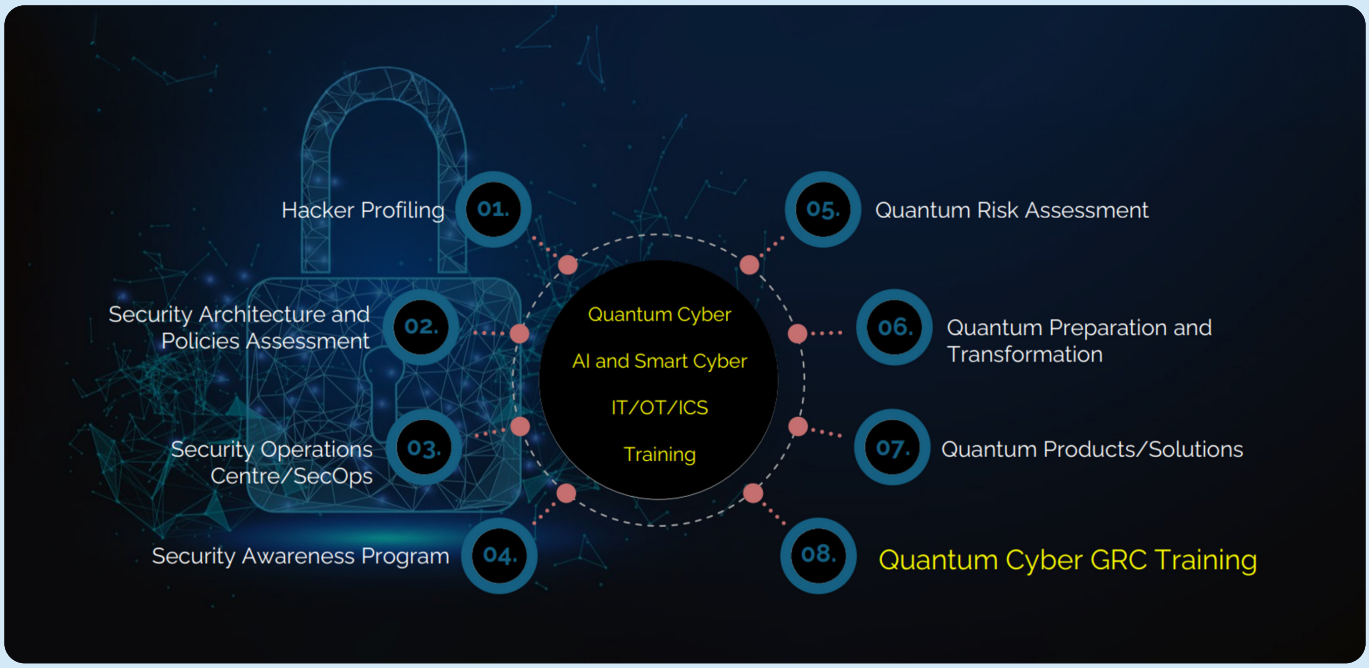



***Figure 1*** *– Quantum Cyber GRC in the context of services available from Cystel*
*Source: Cystel*

> "Quantum computing presents considerable opportunities but also threats. Many industry sectors rely heavily on encryption to protect sensitive information, the exposure of which could cause significant harm to consumers and markets. Addressing this requires a truly collaborative effort to transition to a quantum-secure future."
>
> Suman Ziaullah, Head of Technology, Resilience and Cyber; Financial Conduct Authority

its greater computational power will also overcome the protection offered by many types of encryption systems currently in use. The encryption systems used to underpin many widely-used communications protocols (securing internet connections, remote access, file transfers, and VPNs) and for encrypting enterprise data and emails, are examples that will need to be replaced.

Furthermore, the future threat to encrypted data is an active risk in the present day, for organisations within industries that need to store data for years (because of compliance requirements, or because it is still valid for business reasons). If data compromised now is still valuable or relevant when QC becomes accessible, bad actors can then decrypt and use the data nefariously. Thus, organisations may incur risk at a future date of ransom situations, and compliance penalties, caused by the protection that is in place right now being inadequate.

Cystel's Quantum Cyber GRC services deliver training and tools to enable planning and navigation of the organisation-wide change necessary to counter the threat to current encryption protection from QC.

Four course options are available, for delegates with different responsibilities and perspectives:

- Quantum Cyber GRC Associate, an introduction to management of QC threats from a GRC perspective.
- Quantum Cyber GRC Professional, which focuses more deeply on operational, tactical and strategic best practices.
- Quantum Cyber GRC for Leaders, orienting towards a model that integrates the GRC elements of the technical and organisational change necessary.
- Quantum Cyber Transformation, focusing more closely on putting quantum-ready security in place along with related risk management and policies.

The 'Leaders' option can be delivered over 1-2 days, with a broad target audience: C-level executives; heads of cyber/digital/risk/finance/transformation; and cyber/digital technologists.

## What does it do?

Encryption is a key weapon enabling digital delivery of a huge range of processes and services. It underpins foundational characteristics such as communications, identity, data protection, and privacy, without which the ubiquity of digitally-enabled facilities would be limited due to intolerable risk, and lack of market confidence. This widespread use is the reason that replacing methods of encryption is so fundamental and broad an undertaking for organisations – and also why Cystel recommends a GRC-led approach to any organisation tackling the threat of encryption-related risk increasing.

All types of organisation will have to prepare to upgrade, over time, encryption-enabled technologies that underpin their critical business operations and protect their data assets. Planning how an organisation should navigate that (including minimising disruption, risk, and cost) should involve multi-disciplinary collaboration across all parties internally that could be affected. This is the reason that the training provided by Cystel is relevant to very senior organisational roles, as well as more operational and technical roles. Planning will also involve understanding the related plans of all external suppliers, responsible in most organisations for delivery of many business services and their key technology elements. Those suppliers will typically be integrated digitally in ways which will also require the underlying integration technology to be upgraded, and the supporting commercial agreements may also need to be changed.

Whatever the sequence and scale of events during the upgrade of encryption technologies, numerous risks to business operations and continuity will need to be foreseen and managed. Understanding how each risk can affect individual elements of an organisation differently is a key capability of a GRC approach. Another benefit of the approach is to enable monitoring of technology changes impacting organisational compliance negatively, and to ensure that compliance reporting includes any factors relating to the encryption issues. Organisations should be able to analyse and comprehend these risk and compliance factors of the overall encryption upgrade, including how they apply to different areas of the enterprise, and to be able to summarise them accurately for C-level reporting purposes.

## The bottom line

The problem of quantum computing compromising current encryption methods is an issue for organisation TODAY, not at some future date. Because the use of encryption is so embedded and fundamental, all organisations are prone to incur risk by failing to conduct detailed analysis and plan how to approach the transition to being secure against quantum-enabled compromise of the current technology.

Cystel has in-depth expertise in this niche security area and has invested in capabilities that can help organisations understand and act in the face of this critical problem. Its choice of a business-led focus on the impact and operations during technology transition is key to organisations avoiding unforeseen and costly outcomes.

Bloor believes that Cystel has scope and depth in its capabilities that put it ahead of larger competitors in helping organisations with this present, and ever more pressing, issue.