GQI
Global Quantum Intelligence

Quantum Cyber Security

Post-Quantum Strategic Consulting

www.global-qi.com

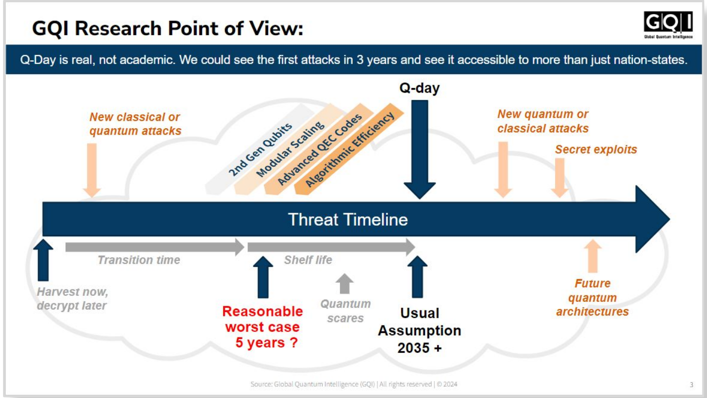
GQI Research Point of View:

The misconception in the market is that quantum tech investments can wait

Misconception 1:
Cryptography will take decades to break!

Misconception 2:
Compliance will follow the threat.

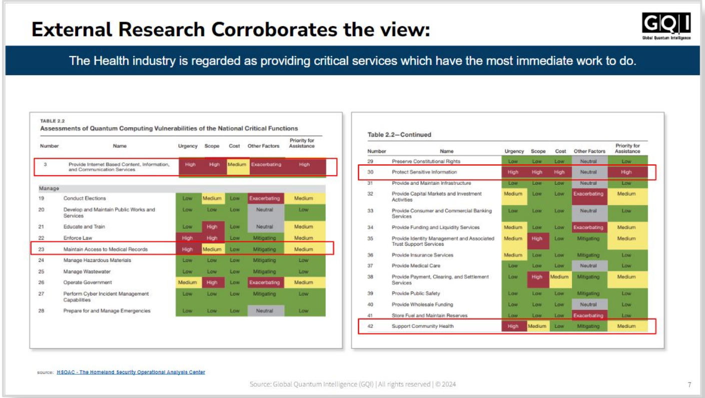
Misconception 3:
Quantum's business utility will take time!



GQI Research Point of View:

Q-Day is real, not academic. We could see the first attacks in 3 years and see it accessible to more than just nation-states.

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024 3



External Research Corroborates the view:

The Health industry is regarded as providing critical services which have the most immediate work to do.

TABLE 2.2
Assessments of Quantum Computing Vulnerabilities of the National Critical Functions

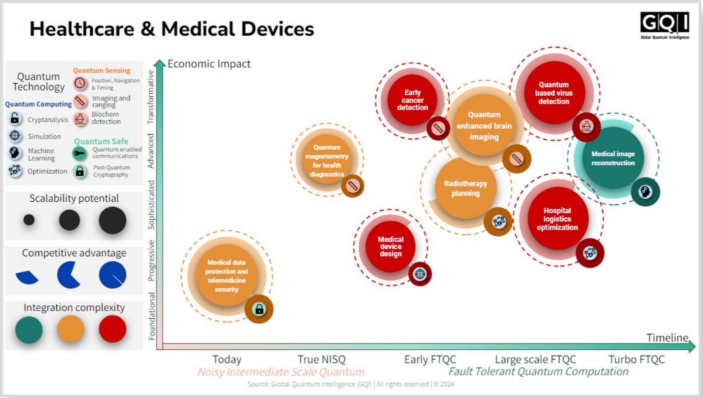
Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
3	Provide Internet Based Content, Information, and Communication Services	High	High	Medium	Exacerbating	High
Manage						
19	Conduct Elections	Low	Medium	Low	Exacerbating	Medium
20	Develop and Maintain Public Works and Services	Low	Low	Low	Neutral	Low
21	Educate and Train	Low	High	Low	Neutral	Medium
22	Enforce Law	High	High	Low	Mitigating	Medium
23	Maintain Access to Medical Records	High	Medium	Low	Mitigating	Medium
24	Manage Hazardous Materials	Low	Low	Low	Mitigating	Low
25	Manage Wastewater	Low	Low	Low	Mitigating	Low
26	Operate Government	Medium	High	Low	Exacerbating	Medium
27	Perform Cyber Incident Management Capabilities	Low	Low	Low	Mitigating	Low
28	Prepare for and Manage Emergencies	Low	Low	Low	Neutral	Low

Table 2.2—Continued

Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
29	Preserve Constitutional Rights	Low	Low	Low	Neutral	Low
30	Protect Sensitive Information	High	High	High	Neutral	High
31	Provide and Maintain Infrastructure	Low	Low	Low	Neutral	Low
32	Provide Capital Markets and Investment Activities	Medium	Low	Low	Exacerbating	Medium
33	Provide Consumer and Commercial Banking Services	Low	Low	Low	Neutral	Low
34	Provide Funding and Liquidity Services	Medium	Low	Low	Exacerbating	Medium
35	Provide Identity Management and Associated Trust Support Services	Medium	High	Low	Mitigating	Medium
36	Provide Insurance Services	Medium	Low	Low	Mitigating	Low
37	Provide Medical Care	Low	Low	Low	Neutral	Low
38	Provide Payment, Clearing, and Settlement Services	Low	High	Medium	Mitigating	Medium
39	Provide Public Safety	Low	Low	Low	Mitigating	Low
40	Provide Wholesale Funding	Low	Low	Low	Neutral	Low
41	Store Fuel and Maintain Reserves	Low	Low	Low	Exacerbating	Low
42	Support Community Health	High	Medium	Low	Mitigating	Medium

source: HSOAC - The Homeland Security Operational Analysis Center

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024 7



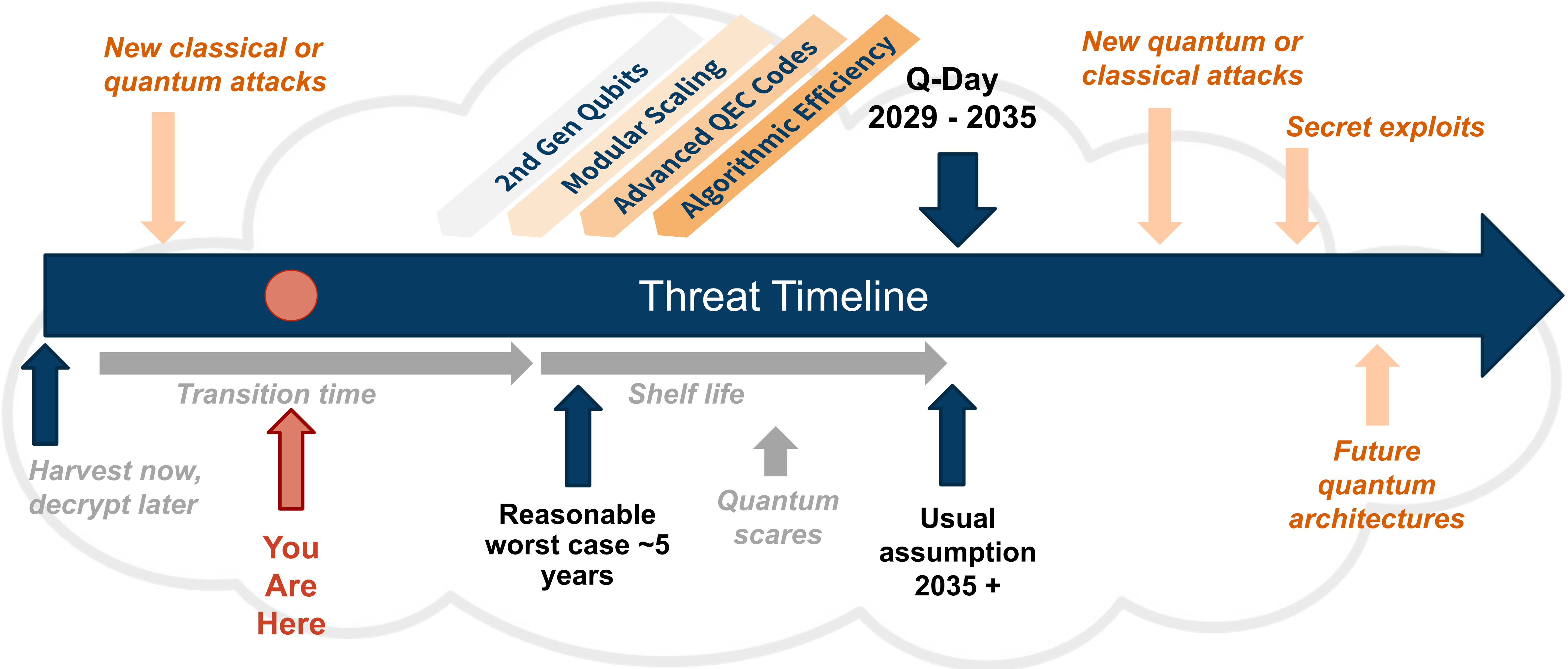
Healthcare & Medical Devices

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Quantum Is Coming:

Q-Day is real, not academic. We could see the first attacks in 3 years and see it accessible to more than just nation-states.



Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Compliance urgency depends on your industry:

The Health industry is regarded as providing critical services which have the most immediate work to do.

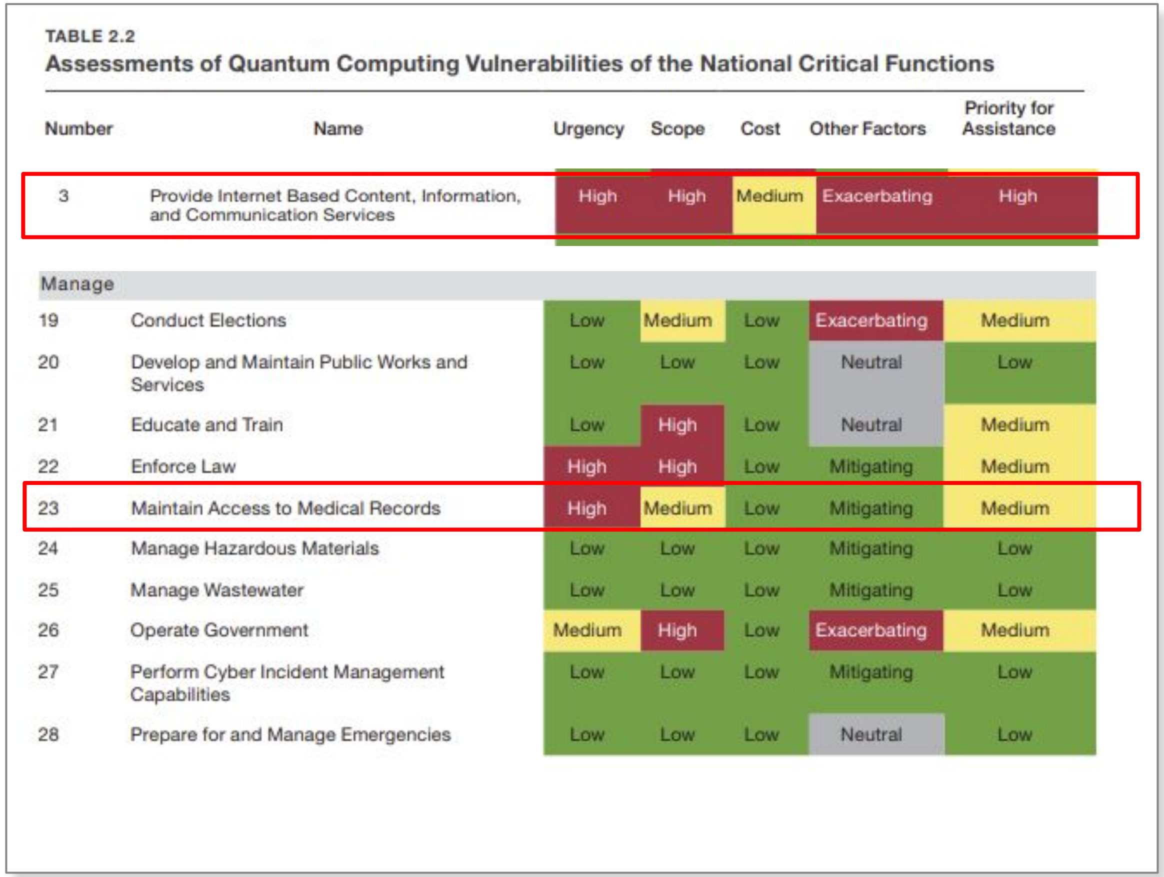


TABLE 2.2

Assessments of Quantum Computing Vulnerabilities of the National Critical Functions

Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
3	Provide Internet Based Content, Information, and Communication Services	High	High	Medium	Exacerbating	High
Manage						
19	Conduct Elections	Low	Medium	Low	Exacerbating	Medium
20	Develop and Maintain Public Works and Services	Low	Low	Low	Neutral	Low
21	Educate and Train	Low	High	Low	Neutral	Medium
22	Enforce Law	High	High	Low	Mitigating	Medium
23	Maintain Access to Medical Records	High	Medium	Low	Mitigating	Medium
24	Manage Hazardous Materials	Low	Low	Low	Mitigating	Low
25	Manage Wastewater	Low	Low	Low	Mitigating	Low
26	Operate Government	Medium	High	Low	Exacerbating	Medium
27	Perform Cyber Incident Management Capabilities	Low	Low	Low	Mitigating	Low
28	Prepare for and Manage Emergencies	Low	Low	Low	Neutral	Low

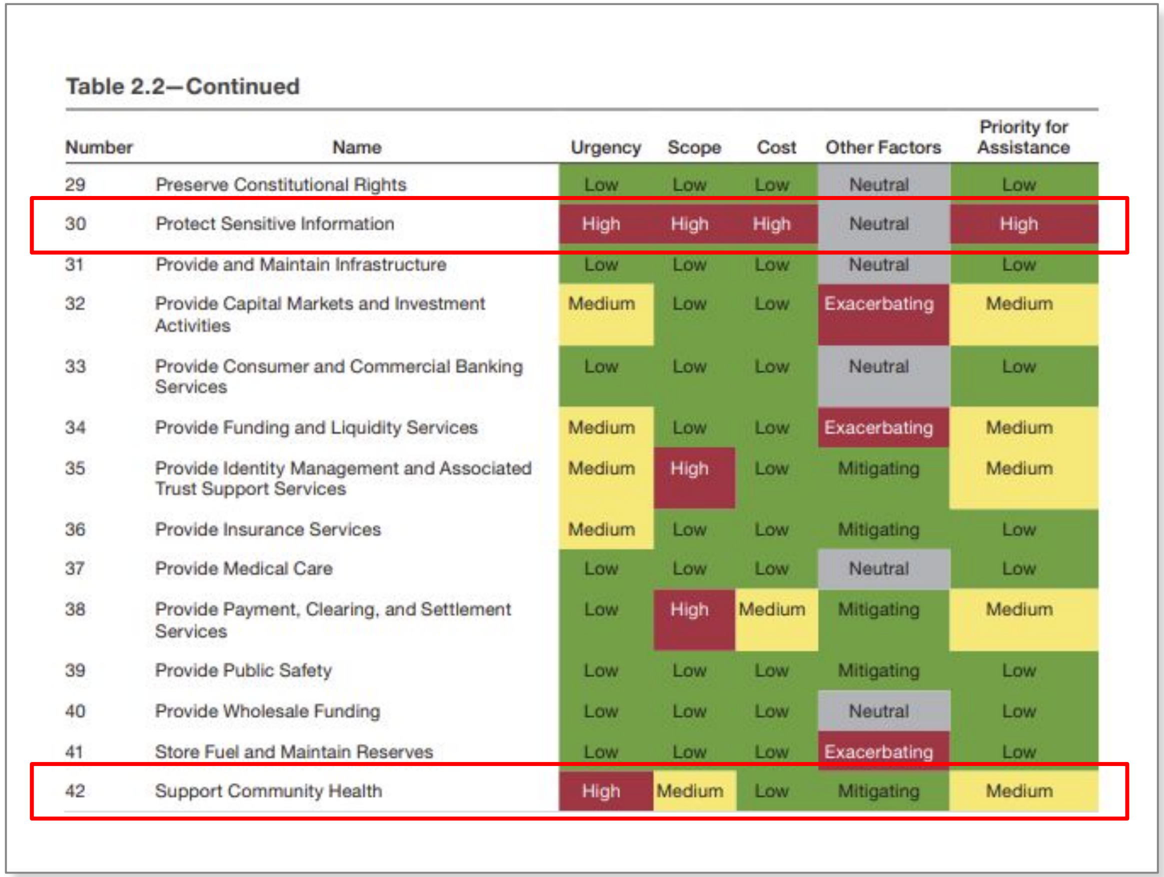


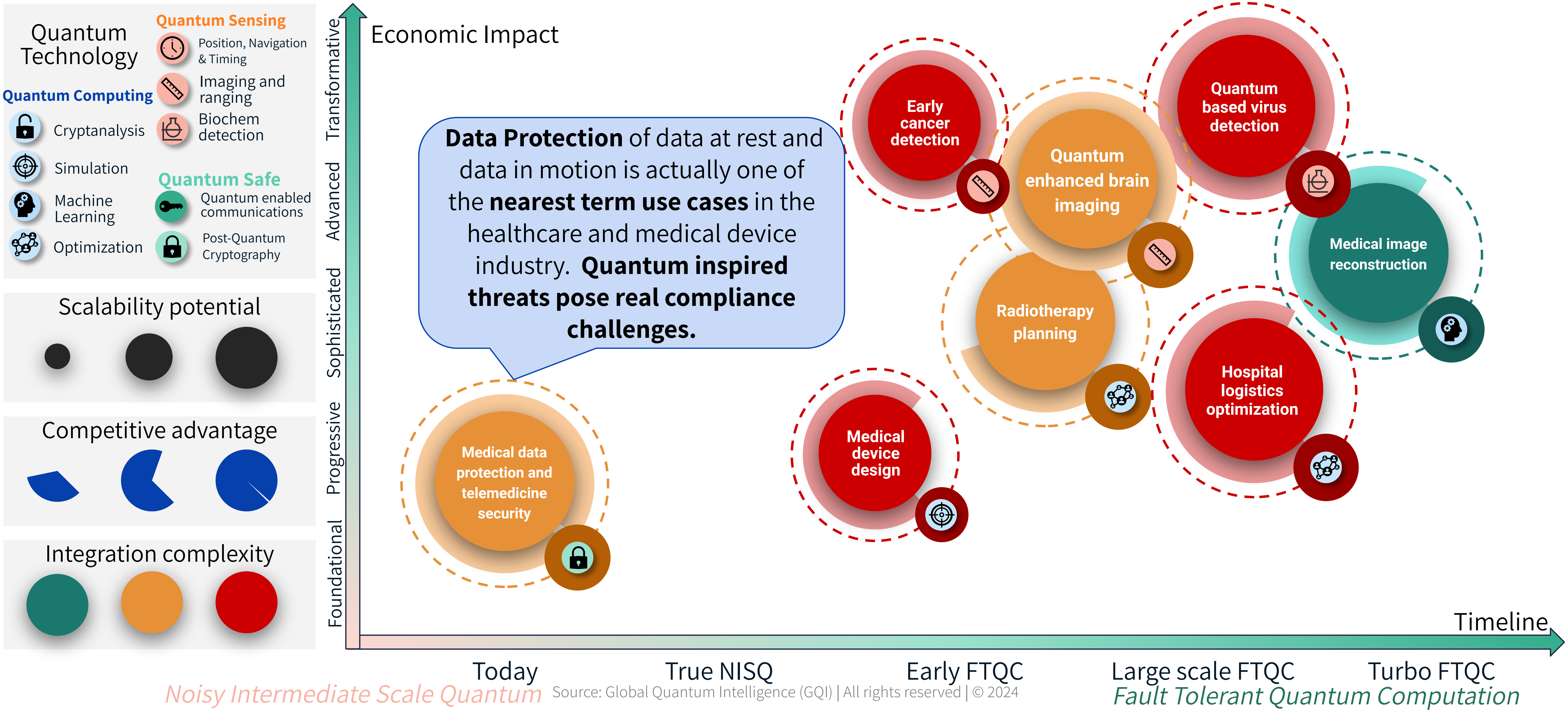
Table 2.2—Continued

Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
29	Preserve Constitutional Rights	Low	Low	Low	Neutral	Low
30	Protect Sensitive Information	High	High	High	Neutral	High
31	Provide and Maintain Infrastructure	Low	Low	Low	Neutral	Low
32	Provide Capital Markets and Investment Activities	Medium	Low	Low	Exacerbating	Medium
33	Provide Consumer and Commercial Banking Services	Low	Low	Low	Neutral	Low
34	Provide Funding and Liquidity Services	Medium	Low	Low	Exacerbating	Medium
35	Provide Identity Management and Associated Trust Support Services	Medium	High	Low	Mitigating	Medium
36	Provide Insurance Services	Medium	Low	Low	Mitigating	Low
37	Provide Medical Care	Low	Low	Low	Neutral	Low
38	Provide Payment, Clearing, and Settlement Services	Low	High	Medium	Mitigating	Medium
39	Provide Public Safety	Low	Low	Low	Mitigating	Low
40	Provide Wholesale Funding	Low	Low	Low	Neutral	Low
41	Store Fuel and Maintain Reserves	Low	Low	Low	Exacerbating	Low
42	Support Community Health	High	Medium	Low	Mitigating	Medium

source: HSOAC - The Homeland Security Operational Analysis Center

Quantum Utility is Close

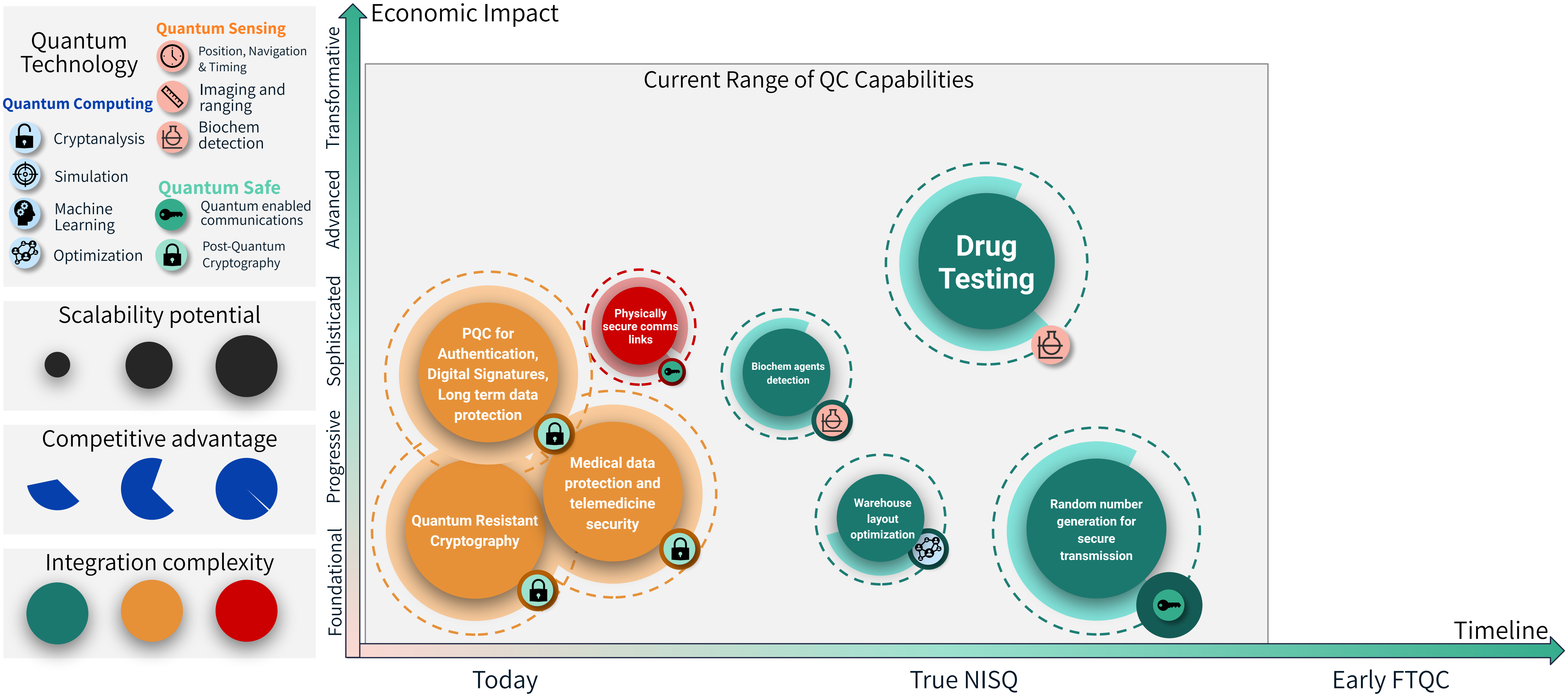
Healthcare Use Cases Highlight Data Protection benefits as soon as Today



Data Protection of data at rest and data in motion is actually one of the **nearest term use cases** in the healthcare and medical device industry. **Quantum inspired threats pose real compliance challenges.**

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Zoomed In View



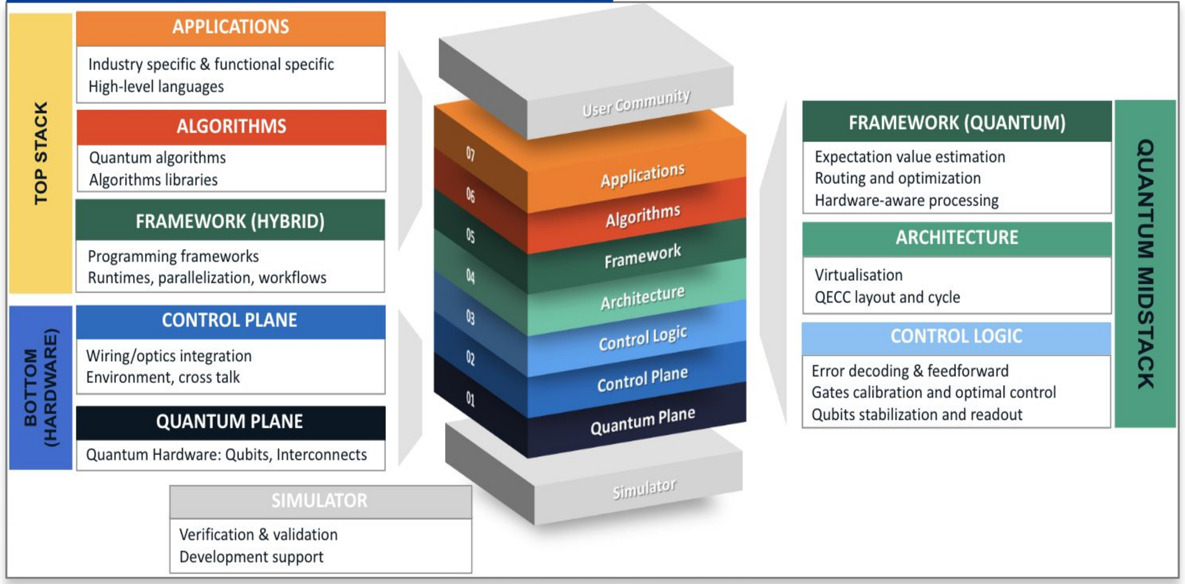
Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

GQI Expertise for you

GQI brings independent, durable frameworks and QRaaS expertise to accelerate your transition to cryptographic agility.

Quantum | AI | ASI | Agentic | Risk & Security | Product

Durable Frameworks



TOP STACK

APPLICATIONS
Industry specific & functional specific
High-level languages

ALGORITHMS
Quantum algorithms
Algorithms libraries

FRAMEWORK (HYBRID)
Programming frameworks
Runtimes, parallelization, workflows

BOTTOM (HARDWARE)

CONTROL PLANE
Wiring/optics integration
Environment, cross talk

QUANTUM PLANE
Quantum Hardware: Qubits, Interconnects

SIMULATOR
Verification & validation
Development support

QUANTUM MIDSTACK

FRAMEWORK (QUANTUM)
Expectation value estimation
Routing and optimization
Hardware-aware processing

ARCHITECTURE
Virtualisation
QECC layout and cycle

CONTROL LOGIC
Error decoding & feedforward
Gates calibration and optimal control
Qubits stabilization and readout

GQI QRaaS Expertise

Compliance	Risk	Cyber Security
Engineering	Cryptography	Product
AI	Architecture	Infrastructure
Data Science	Integration	Automation
Protocols	Devices	Hardware

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Duty of care impels us to start now:

Transition to cryptographic-agility is lengthy, so plan now and build governance championship.

Cryptographic Agility

- Is the ability of a system to switch quickly and easily between different cryptographic algorithms and primitives without impacting SLA.*
- That's just a technical definition. What it really does is reduces business impact risk to disruption, loss, regulatory drivers and reputation.
- More importantly it increases ability to innovate, respond to market changes, improve operational efficiency and integrate (go to market) faster and easier.

Passive Cryptographic Agility

Ability to replace cryptographic libraries without impact to product or SLA. Futureproof product for an easy upgrade path, and end hard coding.

Active Cryptographic Agility

Ability to detect and respond to cryptographic attacks. Monitor and respond within protocol, library, product, portal or data.

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

* https://en.wikipedia.org/wiki/Cryptographic_agility

Get it right or Erode Your Customer Experience and Trust:

Quantum Resilience as a Service (QRaaS) is a critical foundation to preserve your customer experience and trust you have built amidst heightened quantum and quantum-inspired threats

Cryptography in Use

Cryptography in Product

GRC Acceleration

QRaaS Capabilities

- Comprehensive and Automated Cryptographic Risk
- Compliance and Certification
- Analysis & Reporting
- GRC Acceleration

QRaaS Outputs

❖ Fully Automated Cryptographic Risk Detection

❖ Scorecard and Insights

❖ Automated Policy Creation

Approval-ready

❖ Automation of GRC Tasks

❖ Compliance and Standards +

➢ CMMC v2

➢ FIPS 140-3

QRaaS Value Delivered

Reduction in cyber risk, and increased resilience to cyber attack

Fastest time to Comprehensive Cryptographic Insight

Insights into Data Governance

Faster Decision Making by linking to risk context

Improved customer experience through security, response, and uptime

Reduced cost of compliance by ±10%

Insights: Tools, Capabilities and Automation

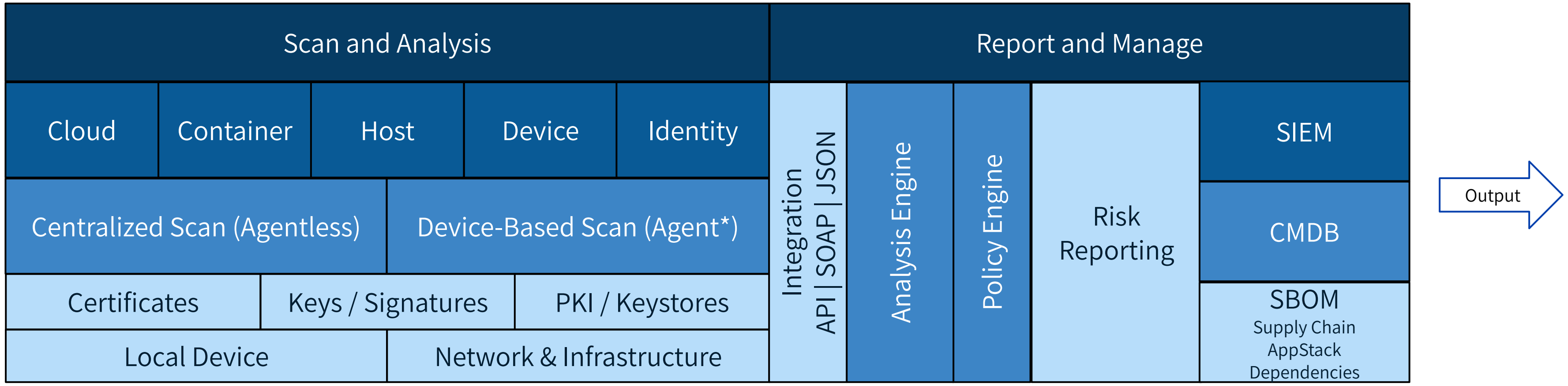
GQI deploys a proprietary and comprehensive toolset to automate and accelerate the analysis process.
We are able to reach into infrastructure, network, device, data and certificate store to determine Risk, Policy, Compliance.

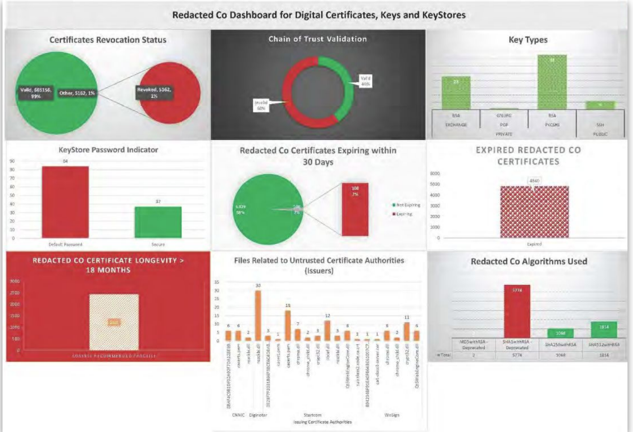
Comprehensive Fingerprinting

Cryptographic Risk

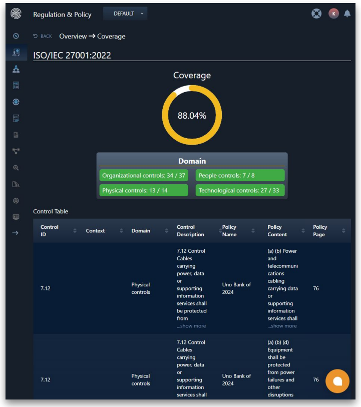
Analysis & Reporting

GRC Acceleration





Scan	Disk *	Network Traffic	AD/LDAP	Codebase	CA	CBOM	SBOM
	Logs	Port *	Protocol *	DB	TPM		



Overview → Coverage

ISO/IEC 27001:2022

Coverage

88.04%

Domain

Organizational controls: 34 / 37

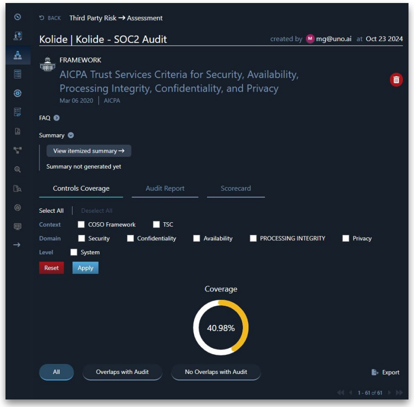
People controls: 7 / 8

Physical controls: 13 / 14

Technological controls: 27 / 33

Control Table

Control ID	Context	Domain	Control Description	Policy Name	Policy Content	Policy Page
7.12		Physical controls	7.12 Control Cables carrying power, data or supporting information services shall be protected from ...show more	Uno Bank of 2024	(a) (b) Power and telecommunications cabling carrying data or supporting information services shall ...show more	76
7.12		Physical controls	7.12 Control Cables carrying power, data or supporting information services shall	Uno Bank of 2024	(a) (b) (d) Equipment shall be protected from power failures and other disruptions	76



Third Party Risk → Assessment

Kolide | Kolide - SOC2 Audit — created by mg@uno.ai at Oct 23 2024

FRAMEWORK

AICPA Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Mar 06 2020 | AICPA

FAQ

Summary

View itemized summary →

Summary not generated yet

Controls Coverage | Audit Report | Scorecard

Select All | Deselect All

Context □ COSO Framework □ TSC

Domain □ Security □ Confidentiality □ Availability □ PROCESSING INTEGRITY □ Privacy

Level □ System

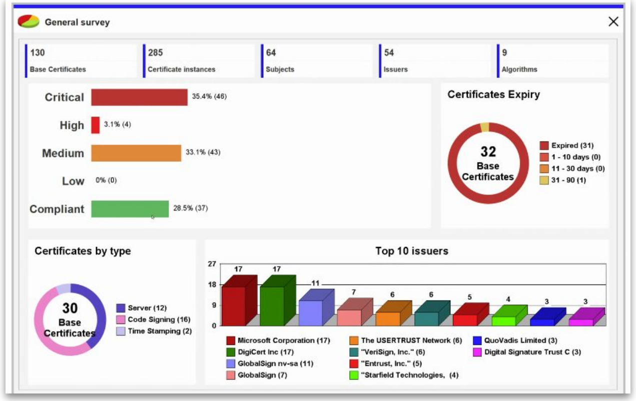
Reset | Apply

Coverage

40.98%

All | Overlaps with Audit | No Overlaps with Audit | Export

1 - 61 of 61


General survey

130	285	64	54	9
Base Certificates	Certificate instances	Subjects	Issuers	Algorithms

- Compliant with Governance Frameworks: ITIL, RISK, PKI, NIST, ISO, etc.
- Built with MITRE Att&ck ® Kill Chain mitigation in mind
- Analysis of Risk from malicious Certificates and CA's
- FedRamp certification and product STIG analysis
- Compliance Acceleration: CMMC, FIPS, CSF, AI RMF

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

GQI QRaaS Accelerates Your Programs and Outcomes

Typical initiatives begin with Quantum Safe Migration and build to Post Quantum Resilience.
“Cryptographic Agility” and “Post Quantum Resilience” require long lived programs and strategic investments.

Quantum Safe Migration

Post-Quantum Readiness

Product Quantum Resilience

Continuous Management

Sample GQI Outputs

Report

Analysis

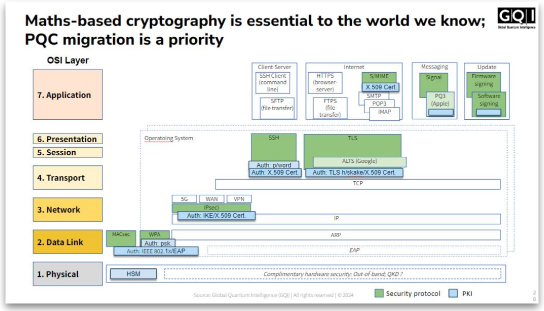
Recommendations

Roadmap

Report

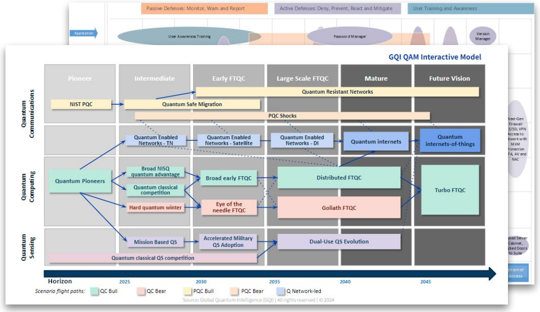
Statement of Work
Post-Quantum Strategic Consulting

Transformational cybersecurity.
Delivered simply.



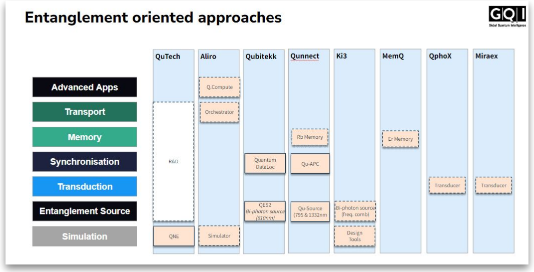
Maths-based cryptography is essential to the world we know; PQC migration is a priority

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024



GQI QAM Interactive Model

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

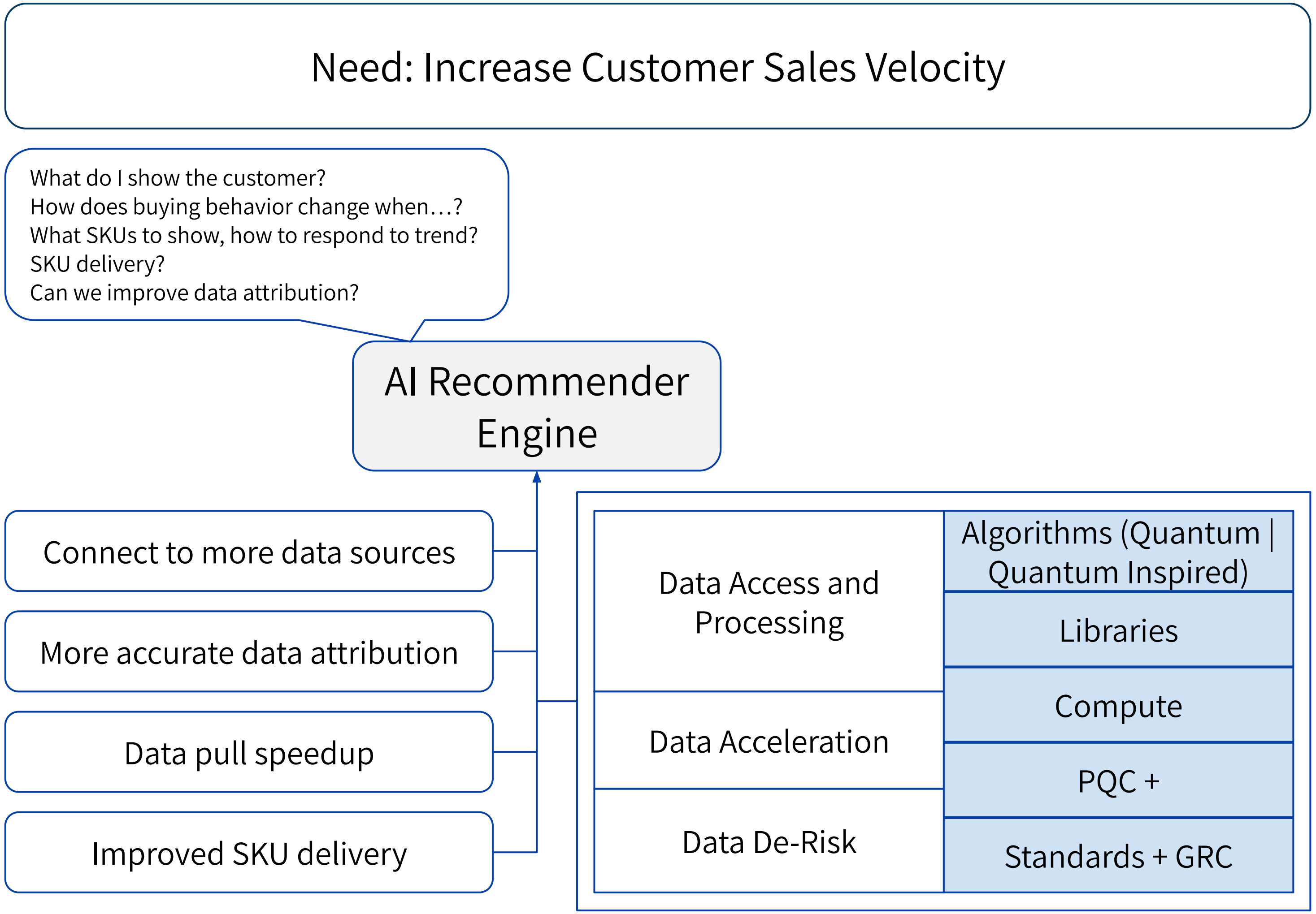


Entanglement oriented approaches

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

AI + Quantum: a Case Study on Revenue Generation

Quantum is a force multiplier for solving real-world challenges. Driving Revenue.



Need: Increase Customer Sales Velocity

What do I show the customer?
How does buying behavior change when…?
What SKUs to show, how to respond to trend?
SKU delivery?
Can we improve data attribution?

AI Recommender Engine

Connect to more data sources

More accurate data attribution

Data pull speedup

Improved SKU delivery

Data Access and Processing

Data Acceleration

Data De-Risk

Algorithms (Quantum | Quantum Inspired)

Libraries

Compute

PQC +

Standards + GRC

Situation: Increase sales velocity in-store and online

Task: Use generative AI to create a recommender engine based on multivariate input to better predict want and recommend products to drive customer sales velocity.

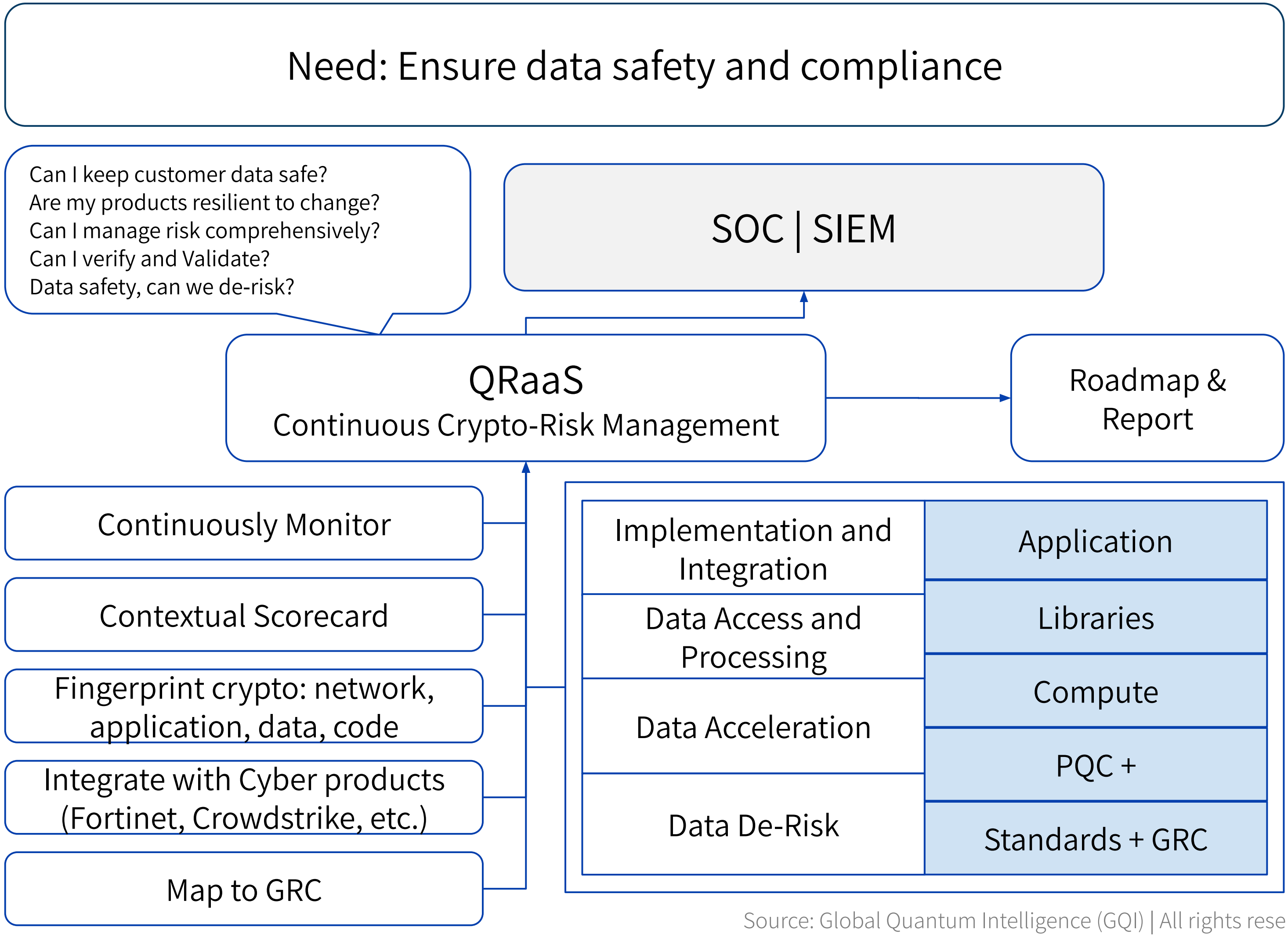
Action:

- Find ways to accelerate AI with quantum
- Determine ways to improve AI training with quantum
- Outline ways to de-risk data with quantum protection
- Create path to improve application resilience with cryptographic agility
- Align on, prioritize, roadmap the effort

Result:
Improvement of AI accuracy to drive better outcomes. Improved speed and reliability of the AI recommender engine. Create in-application agility to standards and policy changes and resilience to attacks.

Security + GRC + Quantum: a Case Study on Risk Reduction

Quantum is a force multiplier for solving real-world challenges. Avoiding Problems.



Need: Ensure data safety and compliance

Can I keep customer data safe?
Are my products resilient to change?
Can I manage risk comprehensively?
Can I verify and Validate?
Data safety, can we de-risk?

SOC | SIEM

QRaaS
Continuous Crypto-Risk Management

Roadmap & Report

Continuously Monitor

Contextual Scorecard

Fingerprint crypto: network, application, data, code

Integrate with Cyber products (Fortinet, Crowdstrike, etc.)

Map to GRC

Implementation and Integration	Application
Data Access and Processing	Libraries
Data Acceleration	Compute PQC +
Data De-Risk	Standards + GRC

Situation: Detect Novel Threats and De-Risk

Task: Understand how cryptography is used in protecting data, network and product, then map it back to GRC and create a path towards resilience.

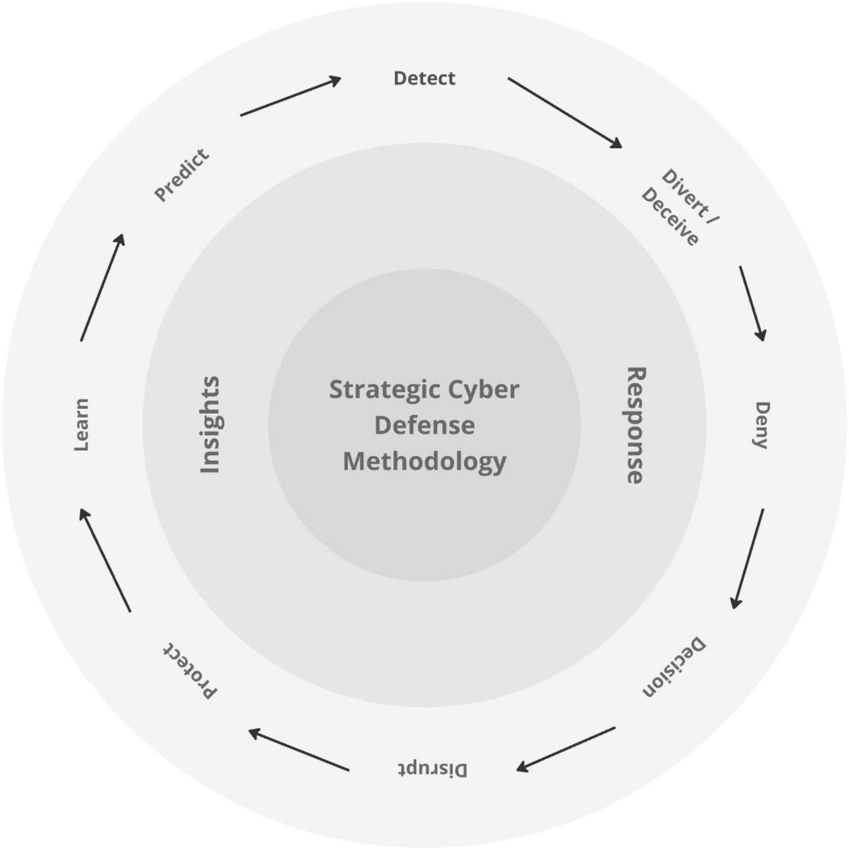
Action:

- Scan and analyze cryptographic risk to IT and infrastructure, application and data
- Determine path to introduce quantum technologies to secure in contextualized manner
- Develop and integration plan to feed information into GRC and Cyber tools
- Align on, prioritize and roadmap the effort involved and create visibility into the process

Result:
Cryptographic risk reduction and business resilience risk reduction in business application agility to standards and policy changes, and improved resilience to attack. Substantive cost reduction in managing the GRC process.

GQI Methodology

Practitioner Driven Approach - GQI marries hands on methods with an asset protection driven mindset. A successful outcome stems from deliberate and defined direction, clarity of action, and verifiable outcomes for business drivers. Our quantum framework is comprehensive, proven and yours.



Faster Insights

Gain visibility into assets protection through the lens of a contextualized risk approach and quantum-level defense.

Better Response

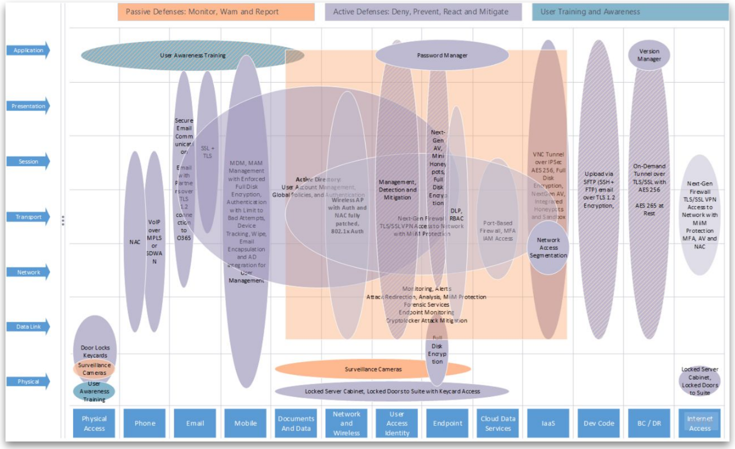
Match actions to appropriate response to risk materialization as defined. Iterate on contextualized risks as quantum innovations arise and implications for Q-Day and related threats increase.

Resilient and Standards Compliant Data

GQI frames the Quantum tech implications in industry standards already in use in your organization.

Application of Methodology

1. Asset Focus
2. Risk and Contextual Prioritization
3. OSI-like Approach
4. Defense in Depth
5. Quantum Resilient Controls
6. Architecture of Protection
7. Automated Learning
8. Education

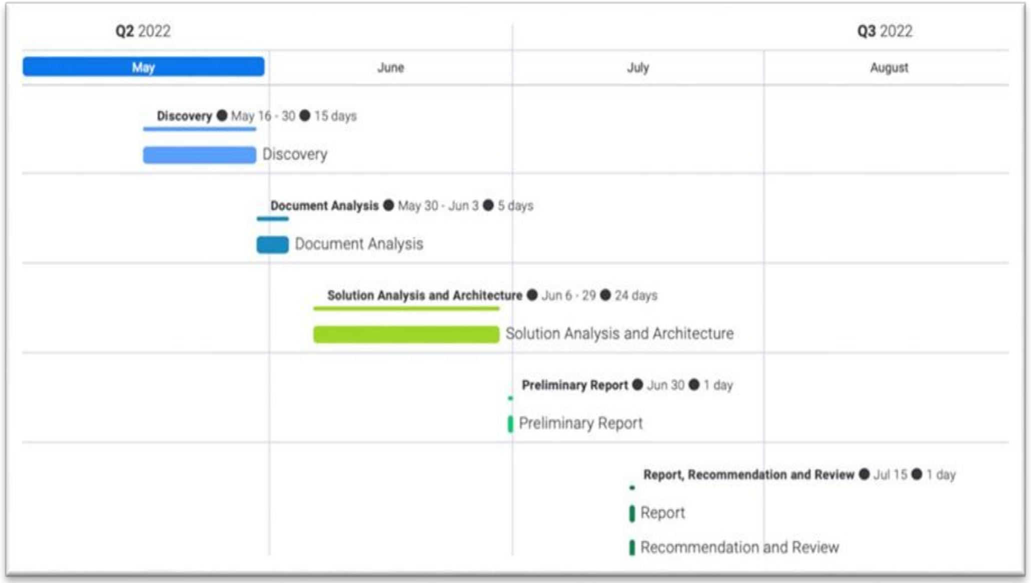


Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Process

Typical assessment projects are short and sharp
8 weeks from kickoff to executive read out, and GQI can tailor the approach to fit the way your organization works.

Milestone	Responsibility	Due Date
Discovery + Scans	GQI + Customer	9/01/2024 ± 9/14/2024
Document Analysis + Scans	GQI	9/15/2024 ± 9/30/2024
Solution Analysis and Architecture	Customer + GQI	10/01/2024 ± 10/21/2024
Preliminary Report	GQI	10/22/2024
Report, Recommendation Review and Acceptance	Customer + GQU	10/28/2024



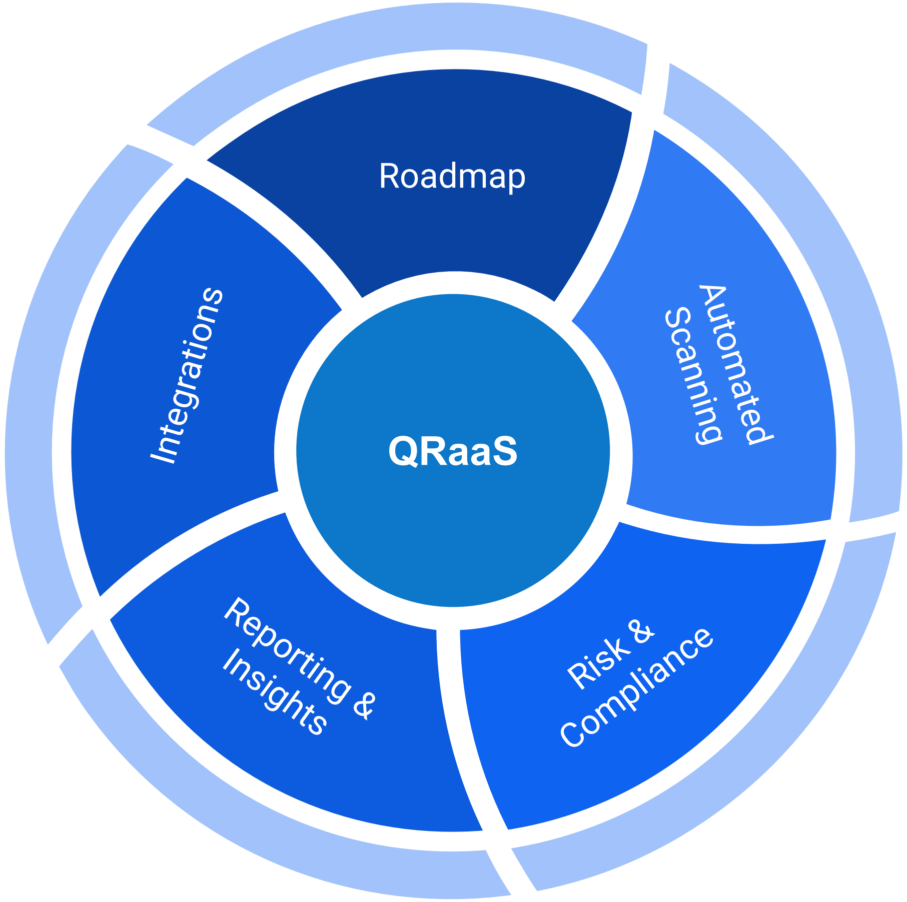
Typical strategy projects are in depth 12-16 week efforts focused on target state development, stakeholder buy-in, initiative development, and consensus on roadmap outcomes across business units

Typical strategic execution projects are months / years of embedded teams and steering committee advisory. Using GQI frameworks, we inform leadership of new quantum developments and contextualize quantum advancements in terms that business can use for rapid decision making.

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Quantum Inside

Quantum Resilience as a Service (QRaaS)



A comprehensive approach to resilience is not a “one and done”

Developing and executing a strategic roadmap involves collaborating with a trusted advisor to understand, contextualize, prioritize, and orchestrate the process. Lean on experience to guide progress, and ensure continuous adaptation to changes.

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Next Steps

1. Align on the right goals
2. Refine understanding of key programs, initiatives, and objectives
3. Set time to regroup on GQI questions and deep dive content
4. Identify and engage additional stakeholders to drive consensus on next steps

Contact

Clay Almy | SVP of Sales
Global Quantum Intelligence, LLC
Washington, DC
202.746.0276 | clay@global-qi.com
calendly | LinkedIn

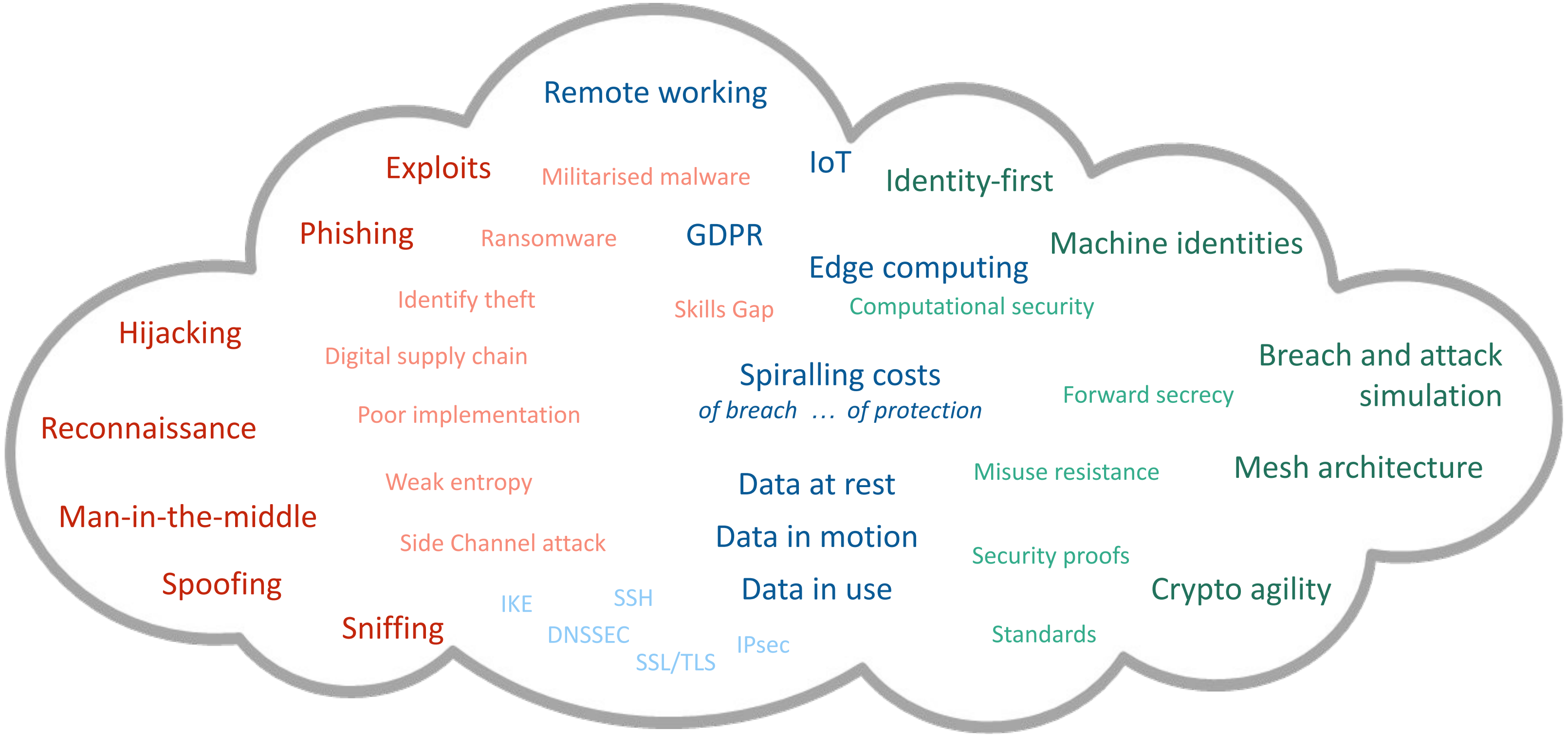
Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024

Security & Product Resilience Needs a Trusted Partner

GQI
Global Quantum Intelligence

The cyber security landscape is already a complex, a cloud of overlapping threats and capabilities. Quantum adds more.

We are help you make sense of Quantum and define contextualized action against this technological complexity.



Remote working
Exploits
Militarised malware
IoT
Identity-first
Phishing
Ransomware
GDPR
Machine identities
Edge computing
Identify theft
Skills Gap
Computational security
Hijacking
Digital supply chain
Breach and attack simulation
Spiralling costs
of breach … of protection
Forward secrecy
Reconnaissance
Poor implementation
Weak entropy
Data at rest
Misuse resistance
Mesh architecture
Man-in-the-middle
Side Channel attack
Data in motion
Security proofs
Spoofing
SSH
Data in use
Crypto agility
IKE
Sniffing
DNSSEC
IPsec
Standards
SSL/TLS

GQI is a Trusted Partner To:

Industry

Microsoft
Google
aws
Mercedes-Benz
SCHOTT glass made of ideas
TREXON
TOSHIBA
Sumitomo
Fujikura

Venture

QUANTONATION
Deep Tech Lab Quantum
NATO OTAN

Government

European Investment Bank
U.S. Department of Homeland Security
QED-C®
مؤسسة قطر
Qatar Foundation
MITRE

Source: Global Quantum Intelligence (GQI) | All rights reserved | © 2024