IMPROVING PROTECTION, SECURITY, AND RESILIENCE

Cybersecurity Capabilities Assessment (CCA)

In today's rapidly evolving digital landscape, safeguarding your organization's assets, maintaining operations, and establishing a robust security ecosystem are of utmost importance. With the ever-present threats of interdependencies, natural disasters, deliberate attacks, and human error, as well as the need to comply with regulatory requirements, your organization needs to stay ahead to thrive. That's where our program comes in.

Quanta Technology's Cybersecurity Capabilities Assessment (CCA) is designed to provide you with a clear understanding of your organization's cybersecurity program, its capabilities, and how well it aligns with your specific needs. We aim to help you quickly assess the current state of your security measures, identify vulnerabilities, and make informed decisions to fortify your defenses.

Overview

The CCA is a comprehensive solution that goes beyond mere diagnosis. By leveraging our expertise and advanced methodologies, we not only assess your organization's security posture but also provide valuable control recommendations.

Our phase-based prioritization of remediation activities empowers you to tackle enhancements in a systematic and efficient manner. We can also help supplement resourcing to fulfill initiatives that are not within your organization's current resource capabilities and/or bandwidth.

The assessment:

- **Involves** power and energy industry advisors.
- **Assesses** eight security program spotlight domains broken into 48 key program capabilities mapped to NIST CSF cybersecurity framework. These capabilities represent activities to establish and mature in the domain.
- **Provides** practical guidance and an actionable roadmap of key program capability activities and relative costs and efforts to close identified gaps.
- **Uses** a right-sized, risk-based, layered approach.
- **Prioritizes** security investments.
- **Distills** complex technical information into a concise, easily digestable executive summary that enables you to swiftly identify areas that require immediate attention.
- **Briefs** executive decision-makers and technical stakeholders via a presentation on the state and direction of the security program.

Program management and governance	Communications and system security	Data privacy and protection	Operations and situational awareness
• Organizational alignment • Strategic risk governance • Resource management • Regulatory and compliance • Policies, standards, and procedures • Measurements and metrics	• Enterprise security architecture • Network access management • Extended enterprise access • Edge device protection • Compute security • Cloud services management	• Data handling and classification • Encryption and key management • Privacy and records • Data loss prevention • Secure data transport • Social media communication	• Asset management • Change control • Vulnerability management • Penetration testing • Event monitoring and correlation • Threat intelligence fusion

Identity and access management	System acquisition, development, maintenance	Incident management and resilience	Physical and personnel security
• Identity management • Authentication and authorization • User provision and deprovision • Privileged access management • Zero-trust and access management • Identity federation	• Supply chain management • Software development lifecycle (SDLC) • Software code review • Deployment and maintenance • Application security testing • Secure code training	• Incident response planning • Investigations and partnerships • Forensics practices • Discovery and containment • Breach response • Crisis management	• Physical security plan • Physical access control systems • Personnel security • Security awareness training • Audit and enforcement • Cyber/physical convergence

PICTURED: Eight security program spotlight domains with 48 key program capabilities

CONTACT US:

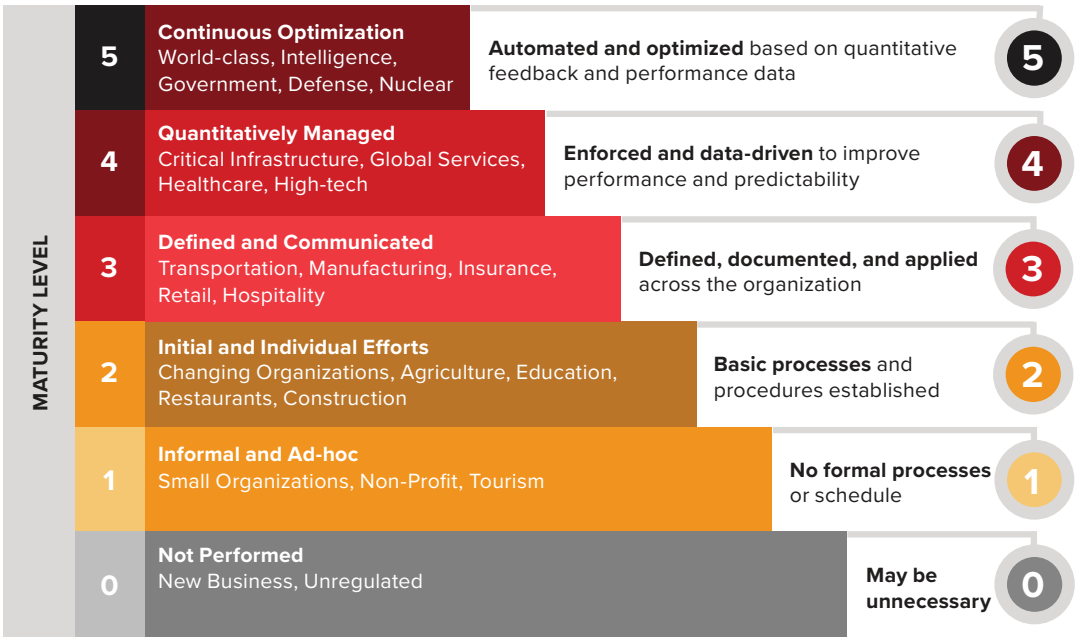
919-334-3000 quanta-technology.com info@quanta-technology.com LinkedIn.com/company/quanta-technology

Cybersecurity Capability Maturity Model (CMM)

The CMM can help organizations of all sectors, types, and sizes evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. Our CMM aligns with industry verticals to ensure a right-sized approach to target maturity and will be used while analyzing each capability.

Cybersecurity Standards and Guidance are Converging

The CCA is designed to take into consideration the IT/OT convergence that many organizations are undertaking. Additionally, critical guidance from NERC, NIST, the Department of Energy, and others shepherds our process to provide a holistic picture of capabilities throughout the enterprise.



Maturity levels build upon and are inclusive of previous levels

PICTURED: Understanding CMM

Rapid, Four-Week Evaluation

Work can be performed remotely, onsite, or via a combined hybrid approach based on your preference.

PICTURED: CCA process

Ensure the Security and Resilience of Your Organization with Our Comprehensive Program

By partnering with us, you can rest assured that you will have a secure and reliable security ecosystem, bolstered by a thorough understanding of your organization's cybersecurity capabilities landscape. With our program's insights and recommendations, you will be equipped to safeguard your operations, protect your valuable assets, and propel your organization towards continued success.

Allow your cybersecurity program to be an asset, not a vulnerability. Embrace our program and empower your organization with the resilience it deserves. Contact us today to get started.

Quanta Technology, LLC
4020 Westchase Blvd.
Raleigh, North Carolina 27607

07/2023, Quanta Technology, LLC

Document number: QTECH-FL-76-X-07-23

CONTACT US:

919-334-3000 quanta-technology.com info@quanta-technology.com LinkedIn.com/company/quanta-technology