QUALITY AND SECURITY DESERVE EQUAL FOCUS IN ICT

The 2024 CrowdStrike outage was a stark reminder of how critical quality is to information and communications technology (ICT) resilience. A faulty software update deployed to millions of devices resulted in widespread system crashes – grounding flights, disrupting government agencies, and halting financial transactions. The economic fallout was measured in billions of dollars, with recovery taking several days for many impacted organizations.

While this was a quality failure, the disruption played out much like a major security breach or DDoS attack – crippling critical services and leaving businesses scrambling to restore their operations. This raises an important question: If the impact of a quality failure can be as devastating as a security breach, shouldn't we be prioritizing quality and security equally when it comes to mission-critical ICT services?

Read the full white paper to explore how a structured approach to quality management can safeguard your organization from expensive disruptions.

QUALITY AND SECURITY: TWO PILLARS OF ICT RESILIENCE

Security and quality are often treated as separate disciplines – managed by different teams, governed by different frameworks, and measured by different benchmarks. But in reality, they are inseparable. A high-quality product must also be secure, and a secure product cannot have quality issues. This correlation is growing increasingly important as today's ICT environments become more complex:

- **Supply chain shifts,** including decoupling from China and reshoring initiatives, will reset everything – with new suppliers, new risks, and new quality unknowns entering the fold.
- **IoT, open-source software, and third-party integrations** have expanded the attack surface to a massive number of devices, increasing exposure to cybercrime and quality issues alike.
- **Cyberattacks are rising,** targeting weak points in both security and quality such as unpatched vulnerabilities, software defects, or misconfigurations.

Quality and security go hand-in-hand, yet many ICT leaders continue treating them as separate issues, duplicating their efforts and implementing distinct standards for each. This may be a product of inertia, where separate quality and security management efforts are ingrained in a company's culture and feel impossible to merge. Or it may be due to the perception that combining quality and security is cost prohibitive. But there's good news: ICT leaders don't need to start from scratch to integrate security and quality.

Some global quality and security frameworks already share a common foundation, making it possible to incrementally build on existing compliance efforts rather than starting over. ISO standards, for example, are designed with this principle in mind – with each step forward comprising just that – a step, not a full reset.

This type of incremental framework makes it efficient and economical to adopt a unified approach to quality and security targeted at keeping mission-critical ICT services online.

TIA'S DUAL APPROACH: SCS 9001 AND TL 9000

To help ICT organizations create a unified strategy for managing quality and security risk, TIA QuEST Forum offers two standards that are built on top of ISO 9001:

- **TL 9000** – A quality management standard designed specifically for the ICT industry, ensuring robust design, testing, and continuous improvement across hardware, software, and services.
- **SCS 9001** – A cybersecurity and supply chain security standard that establishes trusted infrastructure, product/service security, and supply chain protection throughout an ICT product's lifecycle.

By aligning quality and security under a unified strategy, ICT organizations can reduce compliance overhead, improve resilience, and elevate the caliber of their products and services. This combined approach isn't just a theoretical concept, it's a major advantage for your business.

A UNIFIED VISION FOR ICT RESILIENCE

Quality and security aren't competing priorities – they are complementary forces that boost the overall resilience of ICT systems. As the industry faces new risks, now is the time to act. TIA QuEST Forum is setting the standard in integrated quality and security management to help ICT providers support today's mission-critical services and prepare for tomorrow's complexities.

Read the full White Paper to learn how organizations can take a proactive approach to ICT resilience or contact us at membership@tiaonline.org to get involved.

TLBG031525