IS IT TIME FOR THE ICT INDUSTRY TO EMBRACE QUALITY MANAGEMENT STANDARDS?

IS IT TIME FOR THE ICT INDUSTRY TO EMBRACE QUALITY MANAGEMENT STANDARDS?

CONTRIBUTORS:

Ken Koffman, TIA

Mike Regan, TIA

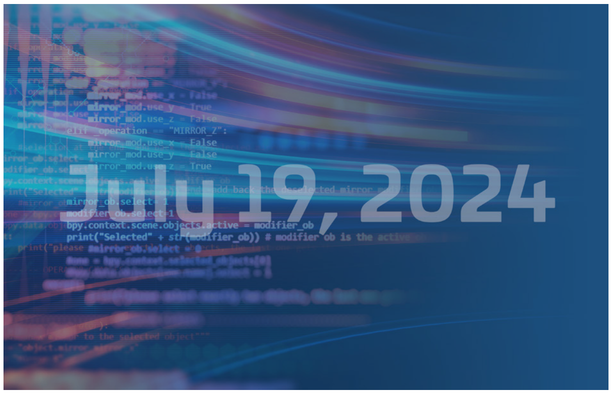
John Wronka, JCW Consulting

INTRODUCTION

Recent high-profile outages in the information and communications technology (ICT) sector have exposed significant vulnerabilities in the quality management practices of IT-driven industries. These disruptions don't just inconvenience consumers; they destabilize essential services like air travel, healthcare, banking, cellular services, and energy grids – creating billions of dollars in economic fallout. While there are many examples of quality-related ICT outages, including the AWS, Meta, and Fastly outages in 2021, the 2024 CrowdStrike outage is examined in this article to help reveal how a single software failure in the ICT sector could impact millions of devices and cause downtime and financial harm.

Industries such as aerospace and automotive have long adopted rigorous quality standards to help prevent critical failures, but even those industries see problems. The TL 9000 quality management standard has greatly benefited the many telecommunications companies that have invested in certification according to our performance data reports (PDRs) and case studies – but the broader ICT industry is lagging in adopting it. We feel that the ICT industry should not wait as this leaves a potential vulnerability for thousands of companies that have not implemented an effective quality system, and it opens the door to both small and large ICT service disruptions.

In this paper, we'll examine the CrowdStrike outage using public sources for information and do not take a stance on causes or liability. We will use the incident as a case study of how implementation of TL 9000, a proven quality framework, can lead to fewer and less catastrophic failures in the ICT industry. We'll review the reported causes and effects of the outage – and reveal several ways that the TL 9000 quality standard could have reduced the occurrence of these incident types while also minimizing their impact on end users. We'll then discuss the quantitative benefits TL 9000 has already demonstrated in the telecommunications sector and explore how TL 9000 can improve profitability for ICT providers through increased quality, customer satisfaction, and continual performance improvement as ICT and telecommunications become inseparable.



THE OUTAGE

On July 19, 2024, The Associated Press reported that CrowdStrike, a large cybersecurity provider, "deployed a faulty update to computers running Microsoft Windows," adding that the "widespread technology outage affected companies and services across industries – grounding flights, knocking banks and hospital systems offline and media outlets off air."

The faulty update was reportedly intended for CrowdStrike's Falcon sensor software. According to CrowdStrike's website, Falcon is "a tiny, single, lightweight sensor that is cloud-managed and delivered" and is "purpose-built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks – including malware and much more."

TechTarget reported that the issue affected over 8.5 million Windows devices worldwide, and it took 10 days to get 99% of the impacted devices back online. The respected cybersecurity researcher Troy Hunt called this "the largest IT outage in history."

The far-reaching impacts of the CrowdStrike outage may have primarily stemmed from the Falcon sensor's role as a central component in endpoint security infrastructure. When the faulty update caused devices to crash, organizations across the globe faced a dual crisis: widespread service disruptions and significant financial losses.

THE IMPACT

The impact of the CrowdStrike outage rippled across critical industries, reportedly leading to over $5 billion in losses based on insurance estimates and highlighting the societal and economic importance of robust ICT systems in a wide range of industries:

- **Healthcare:** Hospitals and healthcare providers faced far-reaching disruptions, affecting patient care and emergency services. These challenges resulted in an estimated $1.94 billion in losses, according to CNN.
- **Banking:** Financial institutions experienced service interruptions, halting transactions and customer access to accounts. The total losses for the banking sector reached approximately $1.15 billion, according to CNN.
- **AirTravel:** Fortune 500 Airlines such as Delta, American, and United had to cancel or delay thousands of flights due to grounded systems, leading to a collective loss of $860 million, according to CNN.
- **Government Services:** Multiple government entities, including the Department of Homeland Security, the Department of Veterans Affairs, the Energy Department, and the Justice Department, reported issues and downtime as a result of the CrowdStrike outage, according to FedScoop.

Beyond financial losses, the CrowdStrike outage exposed vulnerabilities in industries that rely on ICT for day-to-day operations. For large companies and small businesses across sectors, it delayed or halted critical services, created operational downtime, and damaged reputations.

THE REPORTED ROOT CAUSE

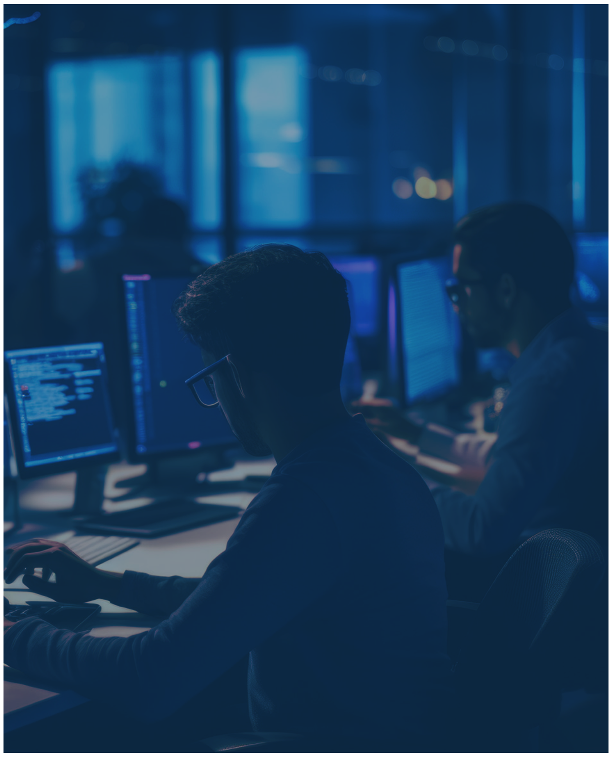
The CrowdStrike outage's root cause analysis (RCA) revealed that the failure stemmed from a mismatch between expected and delivered input fields during a software update, which delivered 21 input fields instead of the 20 expected by the Falcon sensor. This triggered an out-of-bounds memory read and widespread system crashes.

While the company's software development processes included stress testing, the CrowdStrike RCA notes that "tests during development and release builds did not expose the latent out-of-bounds read." And without the ability to quickly roll back the software to a previous version, impacted organizations spent numerous days resolving the issue.

Following the incident, CrowdStrike reportedly implemented corrective actions:

1. **Updating Test Procedures:** New testing protocols, boundary definitions, and software release processes were introduced to identify similar issues in future updates.
2. **Adding Deployment Layers:** A phased rollout strategy was designed to reduce the impact of any potential issues.
3. **Independent Third-Party Review:** Independent software security vendors were engaged to evaluate code and the end-to-end quality process from development through deployment.

This incident and many others underscore the need to fill systemic gaps with proactive quality management. A structured approach to design, testing, deployment, and oversight could have identified and mitigated the risks earlier. This is where TL 9000 offers a critical advantage, with its emphasis on infusing quality management into every step of the end-to-end lifecycle for ICT solutions.



HOW TL 9000 COULD HAVE MITIGATED THE CROWDSTRIKE CRISIS

The CrowdStrike outage revealed systemic gaps in the quality management practices of ICT companies, gaps that could have been addressed by adopting a robust, industry-specific quality standard like TL 9000. While CrowdStrike held certifications for security frameworks such as ISO 27001 and CSA STAR, there was no mention of ISO 9001 or TL 9000 – a notable absence that may have left some risks unaddressed.

Even with effective software development processes, incidents like this demonstrate that certification to a quality management system (QMS) like TL 9000 could have made a difference. While no system can eliminate risk entirely, TL 9000 is designed to significantly reduce the likelihood and severity of such failures while guiding ICT organizations on a path to higher quality. Here's how it could have changed the outcome:

BUILDING RISK MITIGATION INTO EVERY PHASE OF DEVELOPMENT

In addition to fully integrating all the requirements of ISO 9001, TL 9000 incorporates over 80 supplementary requirements that are important to the ICT industry and designed to prioritize quality throughout a product's lifecycle. Beyond mitigating risks, these requirements drive process efficiency and effectiveness, enabling organizations to deliver higher-quality products and services while improving customer satisfaction and profitability. For a software provider like CrowdStrike, TL 9000 certification would have required:

- **End-to-end Process Oversight:** Documenting and managing each phase of software development, from concept and requirements definition to deployment and retirement, ensuring all steps align with defined quality objectives.
- **Rigorous Testing Protocols:** Implementing traceable test plans tied directly to product requirements and documenting results. This includes stress testing and testing under abnormal conditions such as out-of-boundary and invalid input conditions.
- **Release Management:** Establishing controlled conditions for the release of products and documentation to customers.
- **Problem Resolution Processes:** Formalized methods for identifying and addressing defects, allowing for better containment and faster resolution of unexpected issues.
- **Migration Planning Processes:** Ensuring seamless transitions during software updates or deployments, with contingency plans to mitigate risks during system migrations.
- **Change Management and Software Patching Processes:** Standardized approaches to handling software updates, modifications, and patches, minimizing errors and ensuring consistent quality.
- **Software Procurement and Supplier Management:** Defining rigorous criteria for selecting and managing third-party software suppliers, ensuring all external contributions meet quality requirements.

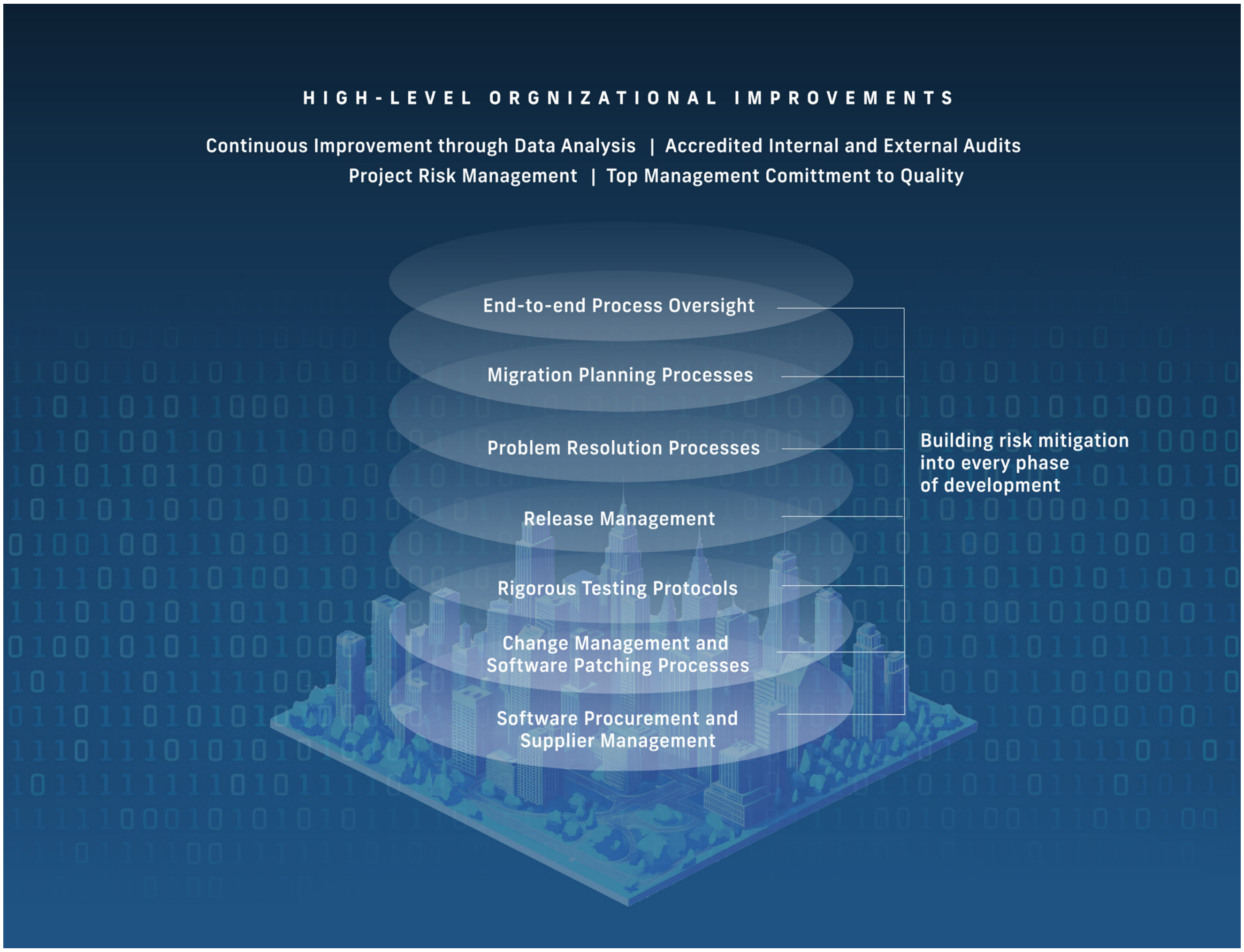
ENACTING HIGH-LEVEL ORGANIZATIONAL IMPROVEMENTS

Beyond operational processes, TL 9000 emphasizes organizational-level actions to foster continual improvement and prevent incidents and outages:

- **Continuous Improvement through Data Analysis:** Certified organizations must collect, analyze, and trend process, design, and development performance data. Key metrics like TL 9000 software fix quality and early software problem reports provide insights into recurring issues, helping teams identify trends and implement improvements proactively.
- **Accredited Internal and External Audits:** Regular reviews by internal audit teams and accredited third-party certification bodies are integral to TL 9000. These audits find weaknesses, identify improvement opportunities, uncover risks, and drive actionable outcomes through root cause analysis (RCA) and corrective actions. These audits are critical to ensuring long-term adherence to quality objectives.
- **Project Risk Management:** TL 9000 emphasizes systematic risk assessment and mitigation at the project level. This structured approach helps organizations preemptively address potential vulnerabilities, preventing small issues from escalating into larger crises.

- **Top Management Commitment to Quality:** Organizational leadership plays a pivotal role in embedding quality as a core value. TL 9000-certified organizations must demonstrate leadership engagement through management reviews, setting clear quality policies, and aligning corporate objectives with continuous improvement initiatives.

With TL 9000 in place, ICT organizations can foster a culture of quality that improves their processes, products and services over time, which can all add up to higher profitability. It also provides multiple layers of protection that keep potential issues from surfacing, spreading, and disrupting customers. Let's examine the CrowdStrike outage as an example of how TL 9000 could have helped prevent, contain, and limit the impact of a software update gone wrong.



HIGH-LEVEL ORGNIZATIONAL IMPROVEMENTS

Continuous Improvement through Data Analysis | Accredited Internal and External Audits
Project Risk Management | Top Management Comittment to Quality

End-to-end Process Oversight

Migration Planning Processes

Problem Resolution Processes

Release Management

Rigorous Testing Protocols

Change Management and Software Patching Processes

Software Procurement and Supplier Management

Building risk mitigation into every phase of development

WHAT IF? HOW TL 9000 COULD HAVE CHANGED THE STORY

The CrowdStrike outage was a wake-up call to the ICT industry. Hospitals, banks, airlines, and government agencies experienced the fallout – all because a single software update delivered one unexpected input field. Devices crashed, recovery took days, and according to insurance estimates, the fallout exceeded $5 billion.

But what if CrowdStrike had been TL 9000 certified? How might the story have unfolded differently? Let's imagine a better outcome – one where a robust quality management framework prevented or mitigated the failure, contained the issue, and protected customers, revenue, and reputations.

PHASE 1: STOPPING THE ISSUE AT ITS SOURCE

In our hypothetical scenario, TL 9000 certification drives CrowdStrike to implement rigorous testing protocols that are well-documented and continuously refined. Before the software update ever reaches production, it is tested against edge cases and abnormal conditions – a core TL 9000 requirement.

Picture the team at work: They simulate everything from corrupted inputs to out-of-bounds data. During one such test, the mismatch between the expected 20 input fields and the delivered 21 is discovered. It's a small detail, but under TL 9000's traceable testing processes, small details don't slip through the cracks. The issue is flagged, the update is fixed, and millions of devices remain online.

PHASE 2: CATCHING THE ISSUES BEFORE THEY SPREAD

Now let's imagine that despite robust testing, the mismatch somehow makes it through. Even then, TL 9000-certified processes prioritize controlled software releases – another safeguard. Instead of pushing the update to millions of devices at once, CrowdStrike rolls it out in a phased, layered and controlled approach.

The update first reaches an internal testing environment or small pilot group. Within hours, crashes occur, but the issue is contained within a controlled environment and only affects a small percentage of the total endpoints. In this scenario, the failure is not only identified quickly, but it's contained and corrected to minimize its impact. Millions of customers remain unaffected.

PHASE 3: CONTAINING THE FALLOUT AND RECOVERING FASTER

Now, let's imagine a worst-case scenario where the faulty update still makes its way to production. Here's where TL 9000's emphasis on documented processes and proactive risk management proves invaluable.

CrowdStrike engineers immediately activate a pre-tested rollback plan – a step that TL 9000-certified organizations routinely create and refine based on continual improvement activities based on the results of their audits. Within hours, devices revert to the previous stable version and business operations resume with minimal disruption.

Under TL 9000, this rollback plan wasn't created in haste. It was developed, tested, and improved long before the crisis emerged. As a result, recovery takes hours. Customers may experience minor hiccups, but there is no prolonged downtime, no widespread economic loss, and no reputational damage.

PHASE 4: BEYOND PREVENTION: DRIVING CONTINUOUS IMPROVEMENT

While TL 9000's processes could have helped prevent CrowdStrike's catastrophic failure, its benefits go further. Regular internal and external audits ensure that processes – from testing to deployment – are consistently applied and constantly refined. Performance metrics like software fix quality and problem reports help CrowdStrike uncover trends before they become risks. Leadership reviews drive accountability and foster a culture of improvement across the organization.

In our hypothetical scenario, CrowdStrike is not just avoiding disasters – it's operating at a higher level. The result? Fewer bugs, faster updates, and happier customers. Costs are reduced. Revenue grows. CrowdStrike bolsters its reputation for reliability and technological leadership in the ICT industry.

A BETTER WAY FORWARD

The CrowdStrike outage cost billions of dollars, disrupted critical services, and revealed systemic weaknesses in quality management. But it may have been prevented. TL 9000 provides a framework for companies to manage risks, avoid crises, protect customers, and deliver exceptional quality.

Imagine an industry where failures like this are prevented before they occur, where issues are caught before they spread, and where organizations operate more efficiently, cost-effectively, and profitably. That's the promise of TL 9000 and certification to the standard.

CONCLUSION

The CrowdStrike outage is one of many and serves as yet another wake-up call for the ICT industry, highlighting the urgent need for a robust quality management framework to safeguard important and even critical systems and services. TL 9000 offers a proven methodology with a track record of transforming the telecommunications industry through continuous improvement, measurable outcomes, and proactive risk management. By embedding quality into every phase of the hardware, software, and service lifecycle, organizations can minimize the likelihood of costly disruptions, protect their reputations, and maintain public trust.

The ICT industry stands at a crossroads. As our reliance on interconnected systems grows, so do the risks of catastrophic failures. The time to act is now – to adopt TL 9000 and elevate the standards for quality and reliability across the sector. This isn't just about preventing the next CrowdStrike; it's about building a resilient future where ICT systems underpin society's most essential functions with unwavering reliability. That's why the TIA has relaunched the TL 9000 working group to update the standard and extend its benefits beyond telecommunications into a wide range of ICT use cases. We encourage organizations of all kinds in the ICT industry to learn more about TL 9000 and get involved.

Don't wait for the next crisis—act now and join the ranks of leading companies that are not only enhancing this standard but also sharing invaluable insights for implementing proven practices. To learn how to get involved contact us at membership@tiaonline.org

DISCOVER THE ROOTS OF TL 9000: A REVOLUTION IN TELECOM QUALITY MANAGEMENT

TL 9000 IN ACTION: REAL-WORLD BENEFITS FOR THE ICT INDUSTRY

The CrowdStrike incident illustrates the catastrophic effects of quality management failures in the ICT industry, but TL 9000 offers a proven framework to mitigate such risks. Since its introduction, TL 9000 has delivered measurable benefits across the sector, demonstrating how a robust quality management system can prevent failures, improve efficiency, and save billions.

THE ORIGINS OF TL 9000: A FOUNDATION FOR INDUSTRY-WIDE IMPROVEMENT

In the early 1990s, rising costs, increasing outages, and expensive incidents prompted major U.S. telecom operators and their suppliers to act. They formed the QuEST Forum (Quality Excellence for Suppliers of Telecommunications), which developed TL 9000 as a telecom-specific QMS. Building on the foundation of ISO 9001:1994 and its later updates, TL 9000 introduced over 80 supplementary requirements tailored to the unique needs of the ICT industry.

What sets TL 9000 apart is its dual focus on:

- **Comprehensive Quality Requirements**: Covering all aspects of design, development, production, and service delivery specific to ICT.
- **Performance Measurement:** Certified organizations must collect and submit monthly data on key performance metrics, such as delivery timeliness, outages, problem reports, and hardware/software returns.

TL 9000's requirements for quality and the measurements it collects work to elevate the entire ICT industry. Each month, QuEST Forum takes all the submitted data, aggregates it, and publishes anonymized industry statistics and trends for comparable product categories. These performance measurements enable certified organizations to benchmark their results against industry averages, best-in-class, and worst-in-class performers. This benchmarking not only drives individual company improvements but also raises the quality bar for the entire ICT supply chain. Over time, these efforts have resulted in tangible, industry-wide quality improvements.

FROM REACTIVE TO PROACTIVE: THE TANGIBLE IMPACT OF TL 9000

TL 9000-certified organizations have demonstrated significant improvements across critical TL 9000 metrics, showcasing the value of a proactive, data-driven approach to quality management:

- **Packet Switches:** A recent TL 9000 study showed a ~62% reduction in major issues and a ~22% reduction in minor issues based on early Software Problem Report (eSPR) measurements.
- **Wireline Software Fix Quality (SFQ):** That same study revealed a ~90% improvement in software fix quality (SFQ) during the period.
- **Wireless Infrastructure:** Hardware return rates improved across five product categories, with one-year return rates (YRR) achieving up to 92% improvement for WLAN Base Station Equipment. The resulting savings reached nearly $1 billion annually, reflecting the scale of TL 9000's impact when applied across large-scale deployments.
- **Smartphones:** Return rates dropped by 35% in two years, reflecting improved product reliability.
- **Edge Routers:** Major problem reports declined by 90% over five years, and defective software fixes fell from 4.5% to 0.2% within 18 months.
- **On-Time Delivery:** Organizations achieved a 130% improvement in delivery performance for edge routers and a 50% improvement for mobile base transceivers over two years.

These results highlight TL 9000's power to not only address specific quality issues but also drive continuous improvement throughout the ICT industry.

ADAPTING TO AN EVOLVING ICT LANDSCAPE

TL 9000's initial success in telecom laid the groundwork for its relevance in today's complex ICT environments. The telecom sector's transition from hardware-driven systems to software-defined networks (SDNs) and virtualized environments posed new challenges – but TL 9000 adapted to meet these demands. Key milestones include:

- **Introducing Virtualized Product Categories:** TL 9000 introduced specialized product categories for virtualization and software-defined systems, ensuring that quality management remained relevant for cutting-edge technologies.
- **Open Source and Multi-Vendor Ecosystems:** With the rise of open-source tools and multi-vendor ecosystems, TL 9000 evolved to include processes that manage quality across increasingly decentralized and interconnected supply chains.
- **Ensuring Consistent Quality in Global Supply Chains:** TL 9000 provided a framework for maintaining quality as suppliers transitioned to contract manufacturing, addressing the complexities of globalized production.
- **Addressing Emerging Concerns:** TL 9000 expanded its requirements to tackle new issues such as cybersecurity and environmental sustainability.

ELEVATING THE ICT INDUSTRY WITH TL 9000

The history of TL 9000 demonstrates how a well-implemented quality management system can deliver measurable benefits that go beyond reducing the likelihood of a catastrophic event. For example, TL 9000-certified organizations have achieved significant improvements in customer satisfaction, with 81% reporting an enhanced brand image, 81% expressing overall satisfaction with the standard, and 74% noting better quality in their products and services. These figures underscore the system's ability to deliver both operational excellence and tangible reputational benefits.

These successes show that TL 9000 is not just a theoretical solution – it's a real-world framework with a proven track record. It empowers ICT organizations to improve process quality, customer satisfaction, and financial outcomes, demonstrating that quality is not just a safeguard but a strategic business advantage.

The same system that reduced costs, improved reliability, and elevated service delivery in telecom can now address the challenges of today's broader ICT sector. As ICT systems become increasingly critical to societal infrastructure, the industry can build on the lessons of TL 9000 to move from reactive crisis management to proactive quality assurance.

JOIN THE TIA QUEST FORUM TO DRIVE INDUSTRY STANDARDS FORWARD

By engaging with the TIA QuEST Forum, you have the opportunity to influence the evolution of quality management standards.

The TL 9000 standard, developed by TIA, is a well-established framework with a track record of success, demonstrated by nearly 2000 certified locations and significant quality enhancements across almost 150 product and service categories.

The TL 9000 Workgroup has been reinvigorated to address the industry's evolving quality challenges, including:

- The rapid growth of sectors like cloud services, the Internet of Things (IoT) with consumer smart devices, satellite communications, and cutting-edge cellular networks such as 5G/6G and ORAN.
- Enhanced capabilities for modern, software-driven operational environments.
- The effects of re-shoring and near-shoring trends, which are reshaping supply chains and facilities, sparking fresh quality concerns.
- New network architectures and technological trends that bring in suppliers who may not have a proven track record of quality in their offerings.
- And more.

Contact us at membership@tiaonline.org

The information and views contained in this paper are solely those of its authors and do not reflect the consensus opinion of TIA QuEST Forum Participants or of the TL 9000 workgroup. This white paper is intended to highlight TL 9000 and the positive outcomes that may be derived from implementation of the standard and acquiring the related certification. This paper is based on publicly published articles that delve into the Crowdstrike issue, and does not take sides or determine fault, for the outage. The only position taken is that TL 9000 represents a proven methodology that if implemented may help companies deliver better products and services. The Telecommunications Industry Association does not endorse or promote any product, service, company or service provider. Photos, products and companies used as examples in this paper are solely for information purposes and do not constitute an endorsement by TIA.

TO JOIN THE QUEST FORUM QUALITY MANAGMENT WORKGROUP OR LEARN MORE ABOUT THE TL 9000 STANDARD

CONTACT

membership@tiaonline.org