qmulos®

EXECUTIVE GUIDE

Rethinking Compliance

Leveraging Compliance to Reduce Risk and Improve Cybersecurity

Cybersecurity compliance is broken, and it has been for a long time.

Despite the world spending more on cybersecurity every year, statistics on compromised data continue to grow. And, even as security vendors and providers deliver more solutions to market, the impact from cyberattacks keeps rising. Globally, there was a 141% jump in the number of records stolen in 2020 – reaching a total of 37 billion, as cybercriminals target more diverse data sources to sell and to use for extortion[1]. Among highly targeted nations, the U.S. has the highest average total cost of a data breach at $9.44 million.

With cybersecurity such a critical and growing issue, **why do enterprises continue to struggle?**

The answer lies in the deep misalignment between risk, security, and compliance. The interconnected and interdependent nature of today's digital economy creates complex matrices of cascading and overlapping risk exposures whose scale and impact run the gamut from local to regional to industry vertical to national. When risk, security, and compliance are treated as siloed initiatives, they fail to achieve their common goal of true cybersecurity.

The onslaught of threat management challenges will continue to get worse and more complex. Legally, the cadence of high profile lawsuits charging companies with false security posture claims will continue to grow. All of this points to a need to **change the status quo before legacy processes become the inherent risk.**

The paper centers on the idea of "Convergence," where Risk, security, and compliance converge for a transformative, effective and efficient approach to managing cyber risk.

Rethinking Compliance

At the core of corporate compliance and enterprise risk management (ERM) lies the idea of deterrence: any compliance actions contrary to those mandated are penalized, and those in adherence are rewarded. This model depends on the organization's ability to detect non-compliance and apply penalties, a challenging proposition in any modern enterprise environment. To be impactful, the detection of non-compliance needs to be timely and accurate, with the resulting penalties sufficiently significant to serve as a motivator for appropriate behavior by both the individual actors and the enterprise at large.

While generally sound, the traditional economic theory underpinning the concept of deterrence loses some certainty when it comes to today's complex multidimensional behavioral models that inform the modern compliance landscape. In short, increased compliance complexity is the reason why detection has become more difficult, and bad actors are exploiting the openings in enterprise security defenses.

Traditionally, compliance mandates have aimed to fortify enterprises against future threats by incorporating historical lessons informed by prior events. The time required by regulatory bodies to develop and publish compliance mandates is counted in years. By contrast, attacker tradecraft evolves daily. This is the first component of the inherent compliance lag.

Another factor contributing to compliance lag is the design of many enterprise compliance management programs, whose workflows tend to reflect original paper-based processes and manual artifact collection methods from decades past. In an always-on age, this approach is no longer viable. Truth is, it hasn't been for a long time.

IN AN ALWAYS-ON AGE, A MANUAL, PAPER-BASED APPROACH IS NO LONGER VIABLE.

[1]Deloitte, https://www2.deloitte.com/ca/en/pages/risk/articles/growing-threat-of-data-breaches.html

Until recently, penalties, the critical element of deterrence-based compliance, have primarily taken the form of fines. When these fines failed to have the desired effect, regulatory bodies have ratcheted up the penalties, hoping to eventually reach a level where compliance can be assured.

In response, compliance has emerged as its own objective, and compliance management as its own function, largely divorced from its intended purpose as a critical tool for managing and reducing risk. Today, enterprises find themselves under increasingly complex compliance obligations, expending significant resources to achieve, maintain, and demonstrate adherence to continuously emerging standards, frameworks, and mandates while failing to actually provide the needed risk mitigation.

For too long, the industry has relied on compliance as the primary means of understanding and managing risk, predicated on the fidelity of the information obtained through often outdated compliance management practices. The cybersecurity industry needs to recognize and remedy the gap between compliance intent and compliance effect. Absent that, enterprises will continue to remain blind to the true state of their security posture.

What this legacy approach has failed to account for is the retrospective posture of traditional compliance programs and their focus on capturing and communicating exclusively historical information.

Traditional compliance reflects the idea of driving forward while staring at a rearview mirror.

A decade ago, Qmulos leaned on its collective knowledge and experience as risk, security, and compliance experts, and asked Is there a better way? Happily, the answer is YES. Compliance-as-we-know-it had to transform. What emerged was the concept of converged continuous risk operations.

A New Generation of Compliance

Compliance that is automated, real-time, and converges the functions of compliance, risk and security is a necessary strategy for evolving legacy enterprise compliance and risk management practices into business-aligned, integrated, modern enterprise and cybersecurity risk management programs. This new era of compliance and risk management leverages the power of big-data analytics and real-time insight to achieve desired risk, security, and compliance management objectives.

This converged, continuous compliance offers a holistic model for cybersecurity and risk transformation that enables enterprises to unlock hidden value in their compliance and security investments. The always-on nature of converged, continuous compliance ensures that today's cyber threats are met with well-designed, effective, and continuously validated security controls. In addition, the efficiencies gained through automation enable critical talent resources to realign from manual data management activities to true risk management decisions. Moreover, automation that leverages today's technology supports a mature, risk-driven, dynamic, and security-optimized enterprise that is future-proofed and equipped to respond to the rapidly changing compliance landscape while equally capable of maintaining business resilience in the face of the continuously evolving global threat landscape.

ZEROING IN ON RELEVANT REAL-TIME SECURITY CONTROLS

"Enterprise leaders who seek to modernize and optimize their risk, security, and compliance programs should consider convergence and automation as key success strategies. Convergence offers significant opportunities to readily leverage current IT and security investments in the context of emerging compliance requirements and evolving risk management objectives. Data-driven automation, focused on common technical controls found in most modern compliance mandates, enables organizations to accelerate their compliance lifecycle, reduce compliance lag, and mature risk and compliance posture."

Matt Coose
CEO
Qmulos

Transforming your enterprise to take advantage of convergence requires leadership to rethink the role of compliance, and recognizing the value of real-time compliance as a force-multiplier for security and risk management functions.

Compliance management practices have been established – and entrenched – over many years. Entire departments have been created to perform tedious and laborious compliance management work. Entire careers have been built around the practice with unique skillsets, roles, and responsibilities seldom found elsewhere in the enterprise.

The value of these activities has likewise been largely confined to the practice of compliance, with limited benefit or value conveyed to other corporate functions. Time and effort poured into compliance is not being reflected in most organizations' security and risk posture, creating a critical gap that must be corrected.

The risk, security, and compliance management challenges facing the modern enterprise have reached a peak point beyond which operating under the current siloed model has become untenable. Stakeholders representing cybersecurity, risk, and compliance operations must come together to transform and advance their organizations' capabilities to meet the challenges of today's advanced cyber threats.

> "Compliance complacency, the industry's broad acceptance of the status quo in compliance management practices, is a major problem. The cottage industry of legacy compliance management solutions and vendor services is incentivized to preserve its well-established revenue models responsible for billions of dollars in annual billings, especially around federal IT and defense industrial base sectors."
>
> **Igor Volovich**
> *Vice President, Compliance Strategy*
> Qmulos

Q-Compliance from Qmulos

Qmulos has been providing next-gen risk and compliance solutions for more than a decade, helping government organizations and large enterprises meet and exceed regulatory requirements, such as NIST 800-171, NIST 800-53, ICS 500-27, SOX, HIPAA, FedRAMP, PCI DSS, and most recently, CMMC 2.0.

Bridging the silos between compliance and security across all data sources and frameworks, the Qmulos platform delivers real-time visibility to risk, security, and compliance operations teams, offering a dynamic view of the enterprise cybersecurity posture at all times. Qmulos Q-Compliance analyzes data from any source in real time to identify compliance gaps and flag potential security weaknesses to keep organizations fully protected.

About Qmulos

Qmulos is a pioneering next-gen compliance, security and risk management automation provider, delivering the innovative power of converged, continuous compliance through its flagship Q-Compliance and Q-Audit technology platforms. Qmulos enables organizations to achieve high compliance confidence while delivering a powerful and engaging compliance experience across all functions and phases of the enterprise compliance lifecycle. Government and industry leaders in the public and private sectors use Qmulos' solutions to ensure the highest levels of cybersecurity.

qmulos.com

qmulos