VENARI SECURITY

Whitepaper

A CxO's guide to Proving Compliance & Taking Reasonable Steps to Protect Data

Mark Slater

Director Channel Sales

Introduction: Why Legacy Technologies Can't Prove Compliance

As a CxO team, you are not only responsible for protecting sensitive data but also for proving to regulators, customers, and stakeholders that your organisation is taking reasonable steps to do so. In today's regulatory and business environment, it's no longer enough to have systems in place—you need evidence that your security measures are working effectively, every second of every day.

However, here's the challenge: existing and legacy technologies were not built to provide this evidence. They can show you have TLS protocols, certificates, and ciphers in place, but they cannot dynamically validate how these elements work together to protect every session and transaction. These systems fall short because:

- They can't monitor in real time. Static audits and manual checks only validate configurations at a single point in time.
- They don't evaluate the interplay of the Trinity. TLS, certificates, and ciphers are checked in isolation, not as an interconnected system.
- They can't meet modern standards. Legacy tools are incapable of aligning with evolving frameworks like NIST and ACSC , leaving gaps in compliance.

To meet your responsibilities as a CxO team, you need new technologies—like Venari's Crypto Assurance—that provide the evidence regulators and stakeholders demand while ensuring your organisation's data remains secure.

1. The Responsibility to Prove Compliance

1.1 Why You Must Prove Reasonable Steps

Every regulation, from GDPR to PCI DSS, requires organisations to take reasonable steps to protect personal and sensitive data. But when things go wrong—such as a breach or an audit—you'll be asked to prove what you did to secure that data.

What Reasonable Steps Mean in Practice:

1. Using up-to-date encryption standards like TLS 1.2 or TLS 1.3.
2. Managing certificates proactively to prevent expirations and disruptions.
3. Ensuring only strong ciphers are used, while weak or deprecated ones are removed.
4. Dynamically validating that these components work together to secure every session.

Without dynamic validation and real-time evidence, you cannot prove compliance, leaving your organisation exposed to:

- Fines and Penalties: GDPR fines can reach €20 million or 4% of annual turnover, while PCI DSS penalties cost $5,000–$100,000 monthly.
- Legal Liability: Without evidence of proactive measures, your organisation may be viewed as negligent in a breach.
- Reputational Damage: Failing to protect data and prove compliance erodes trust with customers, investors, and employees.

1.2 Why Legacy Technologies Can't Prove Compliance

Legacy and existing technologies were designed for static compliance checks, not for providing continuous assurance. They focus on validating individual components (e.g., TLS is enabled, certificates are present) but fail to:

1. Monitor the Trinity Dynamically: They don't validate how TLS, certificates, and ciphers interact to secure every session.
2. Adapt to Modern Standards: Legacy systems can't align with frameworks like NIST or ACSC , which require dynamic and continuous validation.
3. Provide Real-Time Evidence: They can't generate session-level reports showing exactly what was done to protect data at any given time.

What This Means for You:

If your organisation relies on legacy tools, you're left with gaps in compliance, increased risk, and no ability to prove you're taking reasonable steps to protect data.

2. The Regulatory Landscape: Why Proof is Mandatory

As a CxO team, you're responsible for ensuring your organisation complies with data protection and security regulations. Here's why these frameworks demand evidence:

2.1 GDPR: Protecting Personal Data

- Requirement: Article 32 mandates that organisations implement encryption to protect personal data during transmission. Regulators demand proof that encryption systems are maintained and monitored continuously.
- Consequence of Non-Compliance: Fines of up to €20 million or 4% of global annual turnover.

2.2 PCI DSS: Securing Payment Data

- Requirement: PCI DSS (Requirement 4.1) mandates the use of secure encryption standards like TLS 1.2 or higher for transmitting cardholder data.
- Consequence of Non-Compliance: Monthly penalties of $5,000–$100,000, plus potential loss of the ability to process card payments.

2.3 DORA: Operational Resilience for Financial Institutions

- Requirement: DORA mandates continuous monitoring of cryptographic systems to ensure operational resilience.
- Consequence of Non-Compliance: Loss of operational licenses in the EU financial market.

Key Insight:
These frameworks don't just require that you have systems in place—they require evidence that these systems are working to secure every session and transaction. Legacy tools can't provide this evidence, leaving your organisation at risk.

3. The Regulatory Landscape: Why Proof is Mandatory

3.1 GDPR: Protecting Personal Data

- Requirement: Article 32 mandates that organisations implement encryption to protect personal data during transmission. Regulators demand proof that encryption systems are maintained and monitored continuously.
- Consequence of Non-Compliance: Fines of up to €20 million or 4% of global annual turnover.

3.2 PCI DSS: Securing Payment Data

- Requirement: PCI DSS (Requirement 4.1) mandates the use of strong encryption protocols like TLS 1.2 or higher for transmitting cardholder data. The standard also emphasizes the need for advanced monitoring to ensure encryption systems remain effective and aligned with compliance requirements.
- Why Advanced Monitoring is Essential: Without real-time validation, organisations cannot detect configuration drift, expired certificates, or weak ciphers that compromise encryption strength. This leaves systems exposed to breaches and non-compliance penalties.
- Consequence of Non-Compliance: Monthly penalties of $5,000–$100,000, plus potential loss of the ability to process card payments.

Example:
A retail company failed to monitor TLS configurations dynamically, leading to the use of a weak cipher during peak transactions. Hackers exploited the vulnerability, intercepting payment data and triggering $1 million in fines and customer compensation costs. With a tool like Venari's Crypto Assurance, the issue would have been flagged and resolved before it became a breach.

3.3 DORA: Operational Resilience for Financial Institutions

- Requirement: DORA mandates continuous monitoring of cryptographic systems to ensure operational resilience. Financial institutions must provide dynamic evidence of system health and risk mitigation.
- Consequence of Non-Compliance: Loss of operational licenses in the EU financial market, alongside regulatory penalties and reputational harm.

Key Insight:
These frameworks don't just require the existence of encryption systems—they demand evidence that encryption is strong, monitored continuously, and aligned with evolving compliance standards. Legacy tools that focus on static checks can't meet these expectations.

4. Proving Compliance and Building Trust

4.1 How Crypto Assurance Helps You Prove Compliance

1. Evidence for Regulators: Show exactly which TLS protocols, certificates, and ciphers were used to secure every session.
2. Demonstrating Reasonable Steps: Provide dynamic reports that prove your organisation is proactively managing vulnerabilities.
3. Defending Against Fines and Lawsuits: Use assurance evidence to demonstrate compliance and reduce liability in the event of a breach.

4.2 How Assurance Builds Trust

1. Customer Confidence: Assurance reassures customers that their data is protected during every transaction, building loyalty and reducing churn.
2. Investor and Stakeholder Trust: Demonstrating proactive risk management strengthens relationships with investors and stakeholders.
3. Differentiation in the Market: Organisations that can prove compliance and security gain a competitive edge, especially in industries like finance, healthcare, and retail.

5. Call to Action for the CxO Team

Your Responsibilities:

1. Invest in Assurance Tools: Deploy technologies like Venari that provide continuous monitoring, validation, and evidence of compliance.
2. Demand Real-Time Reporting: Require session-level validation and dynamic reports from your IT and security teams.
3. Plan for the Future: Begin transitioning to Post-Quantum Cryptography (PQC) to address emerging quantum threats.

The Bottom Line:
Legacy technologies can’t meet today’s compliance demands or provide the evidence regulators and stakeholders require. With Venari’s Crypto Assurance, your organisation can prove it’s taking reasonable steps to protect data, avoid penalties, and build trust with every transaction.

This revised version uses boardroom language, focusing on compliance, trust, and accountability, while addressing the limitations of legacy technologies. Let me know if you’d like further adjustments!

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.

16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.