

DO BUSINESSES UNDERSTAND THE TRUE COST OF COMPLIANCE?

The compliance functionality in any enterprise is as integral as any cyber security team.

Research conducted by Thomson Reuters indicated that assessing cyber resilience remains a concern among compliance practitioners. However, the research showed that this has seen a reduction in 2022, **55%** expect more compliance involvement in assessing cyber resilience however this was at **62%** in 2021.

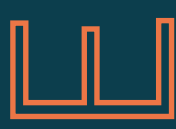
2022 saw an exponential rise in evolving threats - warned the UK Financial Conduct Authority (FCA) - Russian invasion of Ukraine: operational and cyber resilience, March 2022



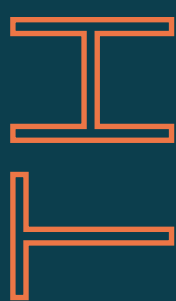
> TAKEAWAYS from our research...



14% of enterprises that participated always maintained compliance readiness.



16% were actually preparing their compliance in line with current demands.



48% of enterprises did track financial investment in tech for compliance; however, only 42% actually track time spent processing usable data.

The QO View



It is a huge misconception that cost only lies in the tech we implement; we must start measuring the time spent by our teams and understand all other associated costs to understand where savings can be made, or investments made better.

True cost analysis lies in measuring all elements of tech and resource time.

Read the full blog [here](#)

Want to learn more about CCM? Take a look [here](#)

www.QuodOrbis.com