resill!on

Assure. Secure. Innovate.

Disconnected by design

The urgent need to replace silos with seamless quality assurance.

The changing face of risk

Across every major sector, the same pattern is emerging. Digital products and systems are becoming ever more complex and interconnected, and more deeply embedded into business operations and our everyday lives.

AI is exploding, offering exciting new possibilities while introducing new avenues of risk. And the regulations overseeing it all are becoming ever more stringent and the bodies more active.

Assurance functions, aimed at making sure products work safely, securely and as intended, remain stubbornly disconnected, even as the risks multiply and converge. As analysis from Resillion and their partners indicates, this is fast becoming a major cause of concern for company leaders.

If you thought the responsibility for addressing all of this begins and ends with your in-house testing teams, it's time to think again. Whether you operate in consumer electronics, banking, energy and utilities, or anywhere in between, operational assurance and throughout the digital lifecycle is critical.

Getting it right can reduce your spending on costly development cycles, improve reliability, and get your products into market faster. But get it wrong and business-critical operations are put at risk. Every new launch, update or integration then carries wider risks to both revenue and reputation – from internet-connected televisions and warehouse sensors to digital banking platforms and remotely managed wind turbines.

90%

90% of enterprises said they're looking for a more connected approach.

The problem here isn't innovation. It's isolation. Most enterprises still manage quality assurance/quality engineering, enterprise cyber security, and conformance and compliance as separate worlds. This approach made sense when systems were simpler and failures stayed local. But not anymore.

An interoperability issue can derail an energy grid upgrade. A performance fix can introduce a vulnerability that spreads through a connected device ecosystem. A change in a third-party API can break an entire banking journey overnight. And, as we see every day, the impacts of a successful cyber breach are onerous for both the business and its customers.

This is how internal issues become external crises – everything from operational disruption and costly recalls to uncomfortable front-page headlines.

Leaders are already exploring alternatives. According to extensive analysis commissioned by Resillion, 90% of enterprises said they're looking for a more connected approach to assurance across quality, security and conformance for both their enterprises and their products. Not because it's a technical optimisation (although it is) but because fragmented assurance processes now threaten business operations, delivery speed, customer experience and, ultimately, revenue.

This paper explores why the old approach is broken in today's interconnected world, and how a single system of assurance offers a more predictable and resilient way forward.

Why assurance needs to change

Nobody sets out to build poor practice into their organisation. Most of the time it's simply what they inherit.

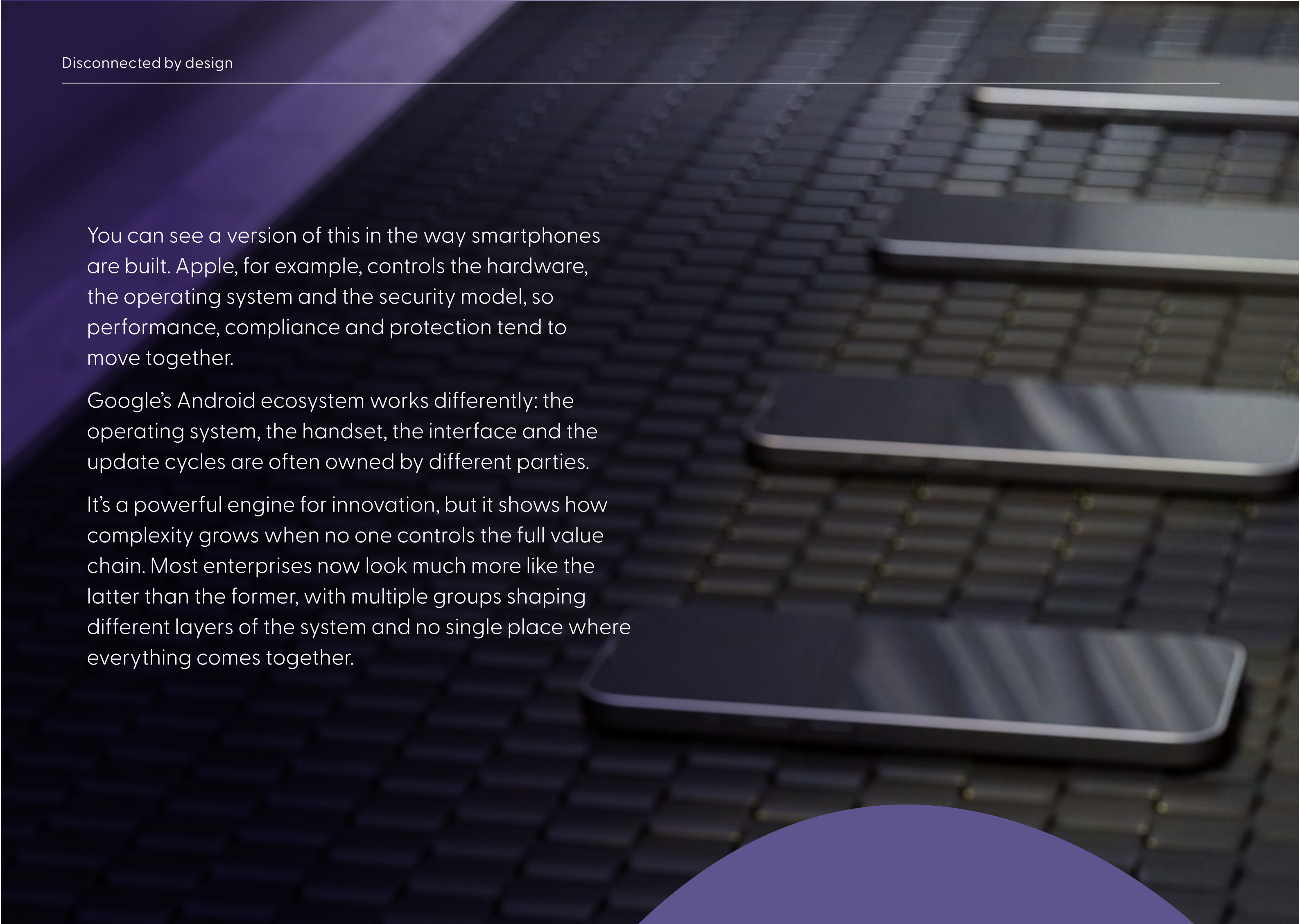
Each team has built its own way of working, its own tools and its own idea of what "ready" looks like. Over time, that becomes the culture.

None of this happens because people aren't doing their job. It happens because, all too often, each team focuses on their own part of the the operations or development lifecycle. And there's rarely a KPI around collaboration. The challenge is amplified in integrated software and hardware systems, where conformance, quality assurance and cyber security each see a different part of the picture, but rarely the whole.

In many organisations, these departmental silos are the rule rather than the exception. Teams working on the same product often operate with little connection to 'the next step'. A security group may assume quality engineering has validated a control. Quality engineering may be unaware of a new cyber threat. Conformance may expect a check that nobody upstream has built into the design or test plan. It isn't resistance so much as distance. Teams don't talk because the structure doesn't ask them to.

It's also a question of heritage. Digital-native organisations tend to bring these disciplines together instinctively. They're also more likely to treat software and physical systems as a single, integrated whole, rather than separate domains to be assured in isolation. In contrast, more established players often have older operating models under the surface, and those models shape how work flows even as the technology changes around them. Companies naturally think of themselves as a single unit, but they behave more like disconnected ecosystems, and an ecosystem is only as strong as its weakest link.

> "The problem isn't effort or intent. It's that teams are measured, rewarded and organised separately, so no one owns what happens in between."
>
> **Yaron Kottler**
> CEO & Chairman, Resillion



You can see a version of this in the way smartphones are built. Apple, for example, controls the hardware, the operating system and the security model, so performance, compliance and protection tend to move together.

Google's Android ecosystem works differently: the operating system, the handset, the interface and the update cycles are often owned by different parties.

It's a powerful engine for innovation, but it shows how complexity grows when no one controls the full value chain. Most enterprises now look much more like the latter than the former, with multiple groups shaping different layers of the system and no single place where everything comes together.

> "Organisations haven't ended up with fragmented assurance through neglect, rather through operating models built for a different era. And the business consequences are very real: delayed launches, costly redesigns, inconsistent compliance and exposure to fast-moving cyber risks."
>
> Yaron Kottler,
> CEO, Resillion

Wider issues creating more problems

Global dynamics make this disconnection even more challenging. Requirements shift quickly and a supplier may still be delivering to an outdated standard without realising it.

A regulatory change that's understood in one part of the organisation might never reach the team responsible for a critical component. And as AI-generated code and automated tooling become more common across suppliers, new errors can enter the system long before anyone sees them.

By the time an issue is identified, the product is often heading for final testing or launch, or the business operations are already compromised.

Today's sophisticated cyber security risks compound the challenge. Anything with an IP address becomes an attack surface the moment it goes live, whether it's a household device, an industrial sensor, an electric vehicle (EV), or the charging point it relies on.

If the 'endpoint' isn't fully protected there's a problem – and this increases with the interconnected nature of supply chains. An EV, for example, now ships as a software platform, its security depending on components built by dozens of suppliers, all updating at different speeds. A small oversight upstream can ripple through an entire ecosystem.

Time to rethink the approach?

Across sectors, the pattern's the same. Teams don't ignore each other; they simply operate inside structures never designed for this level of interconnection.

Each function sees its responsibilities clearly, but issues emerge in the interactions between them – where performance affects security, where security affects compliance, where compliance affects usability. In short, in a world where innovation now outpaces oversight, organisations need to rethink how assurance works.

In a world where innovation now outpaces oversight, organisations need to rethink how assurance works.

Modelling an integrated future

As we've seen, fragmented assurance leaves too many moving parts and too little visibility, but the answer isn't another layer of governance or a bigger testing team.

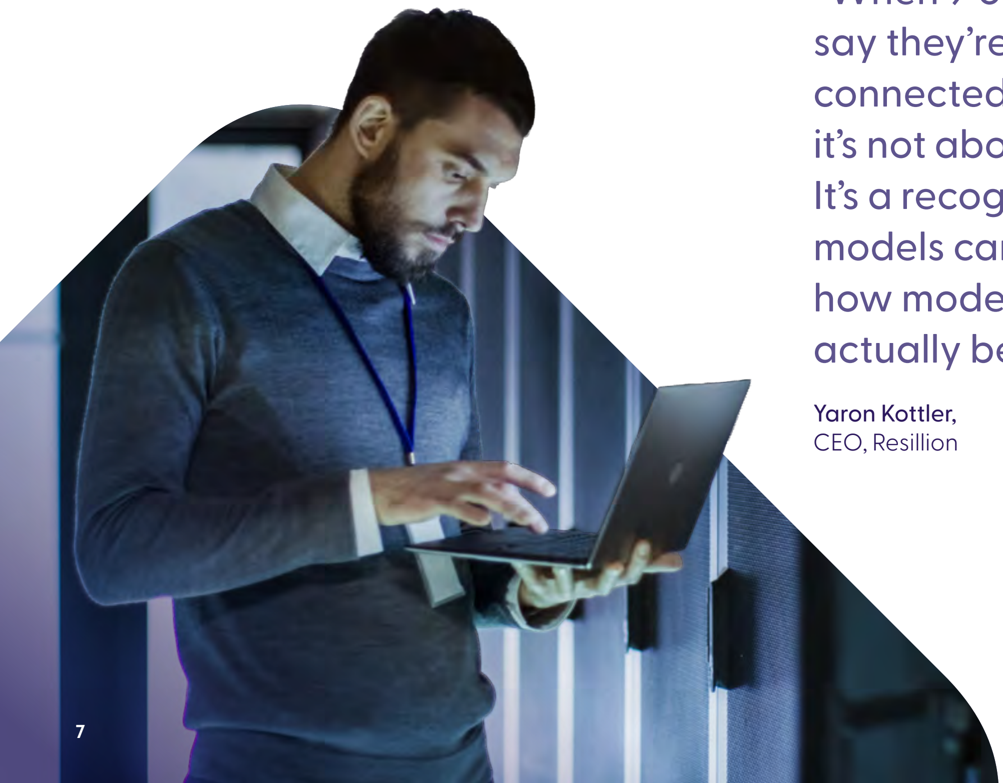
It's about breaking down siloed thinking – and moving towards a more connected, single system of assurance.

Here, the disciplines that determine product readiness are brought together into one connected model across the lifecycle. Work stops being a chain of handovers and becomes a continuous flow of shared requirements, shared evidence and shared decisions. Instead of discovering conflicts late – a performance fix that weakens security, or a security change that breaks compliance – teams can see these interactions earlier, when they're easier to resolve.

In practice, this means making a shift left and getting earlier visibility of changes.

A performance update, for example, can be checked for any security consequences while it's being planned. New compliance requirements reach the people who need to build around them rather than appearing late in the process. And because security is built in (not bolted on) from the very beginning, potential vulnerabilities that appear during development – or worse, after release – are dealt with as a natural part of the development process.

Crucially, it also means shifting right; using insight from live operation, incidents and change to improve how systems are designed, tested and governed over time. This includes how systems are adopted, used and supported by people in real operating conditions.



> "When 9 out of 10 organisations say they're looking for a more connected approach to assurance, it's not about tools or process maturity. It's a recognition that fragmented models can no longer keep pace with how modern products and systems actually behave."
>
> **Yaron Kottler,**
> CEO, Resillion

A structure built for today

This new approach matters because the environment around digital delivery is shifting fast. Release cycles are shorter, user expectations are higher and regulations evolve quicker than many teams can track. A single system of assurance gives organisations a structure that can keep pace; closing gaps and making issues visible before the product, upgrade or system goes live.

The benefits of a connected approach:

Compliance by design. Standards and regulation are embedded from the start, ensuring continuous readiness for CRA, DORA, and the EU AI Act.

Earlier insight, faster delivery. Unified testing and security validation catch issues sooner, validating readiness and accelerating release cycles.

Continuous improvement. Post-launch insight linked across connected assurance disciplines.

Smarter governance and accountability. Integrated data and shared metrics give leaders clearer visibility into performance, risk, and compliance maturity.

Lower cost and complexity. Integration cuts inefficiency across teams, tools, and suppliers, reducing cost of delivery and cost of failure.

Leaner operations. Unified assurance processes and shared insight improve decision-making across the lifecycle, from development through live operation.

Resillion's extensive research and analysis has identified that many leaders are already heading in this direction. Treating assurance as one connected discipline is simply a more reliable way to run modern systems. The question isn't whether this shift is coming. It's how to make it work in practice.

Thanks to BCG for contributions to the analysis in this report.

Defining a single system of assurance

A single system of assurance connects cyber security, and conformance and compliance, quality assurance and quality engineering across business operations and product development, into one continuous workflow.
It replaces handovers with shared requirements, data and decisions.
Each discipline retains autonomy, but performance, standards and security are integrated from the very start.

Total Quality:

Assurance from the inside out.

If a single system of assurance is the direction of travel, Resillion's Total Quality model offers a way to operationalise it.

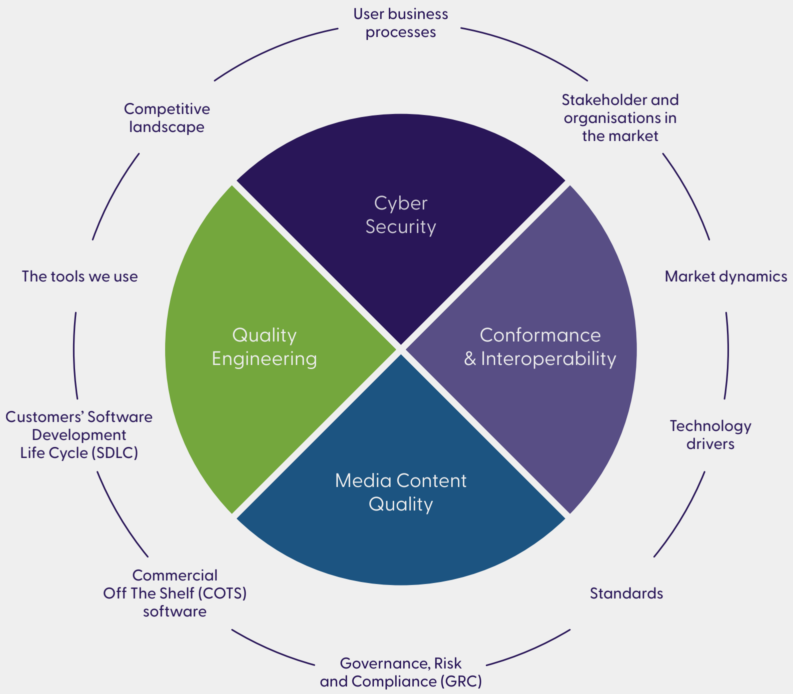
It brings quality assurance, cyber security and conformance and compliance together as one continuous workstream rather than a set of disconnected activities.

Here, each discipline brings a different perspective, from software behaviour and physical integrity to security exposure and regulatory expectation. Now, instead of each team working to its own plan, they work from the same requirements and evidence. So it becomes much easier to see how a change in one area affects another, and to deal with issues earlier rather than rediscovering them late in the cycle.

> "You don't experience quality or security in design documents. You experience them in day-to-day operation – through how products and systems are used, supported and changed under pressure."
>
> **Yaron Kottler,**
> CEO & Chairman, Resillion

Total Quality also goes further than just integrating these disciplines. It covers both the full lifecycle - from build and delivery through to live operation, not just development – and the full business operations and ecosystem. Testing and quality assurance sit alongside monitoring, remediation and recovery. While cyber audit, forensics and advisory work sit alongside compliance testing, inspection and certification.

Total quality across the digital lifecycle


User business processes
Stakeholder and organisations in the market
Market dynamics
Technology drivers
Standards
Governance, Risk and Compliance (GRC)
Commercial Off The Shelf (COTS) software
Customers' Software Development Life Cycle (SDLC)
The tools we use
Competitive landscape
Cyber Security
Conformance & Interoperability
Media Content Quality
Quality Engineering

Assurance now shifts left to the earliest design decisions, so performance, security and compliance requirements and testing are built in before they become hard to change. It shifts right into live operation, using real-world behaviour, monitoring and incident insight to strengthen systems over time. And, increasingly, assurance shifts outwards, too – extending beyond individual teams or products to suppliers, partners and the wider ecosystem. Because today's products are defined by how they connect and interact with other systems, platforms and services – and assurance has to reflect that reality.

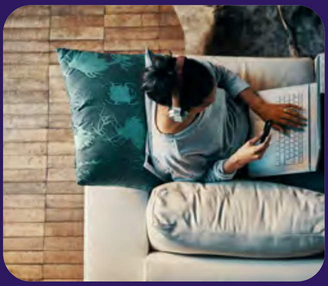
Crucially, this also goes beyond engineering alone. Even the best-designed systems are exposed to operational realities – from human error and credential compromise to issues introduced during manufacturing, deployment or change.

Left unaddressed, these gaps increase risk, drive inefficiency and undermine delivery speed and time to market. Total Quality recognises that assurance therefore has to extend across people, processes and physical production, not just software design.

This changes how organisations operate. With Total Quality, you can pre-determine many conformance and interoperability outcomes by aligning requirements, evidence and validation earlier in the process. It uses automation, tooling partnerships and AI where they make work faster or more reliable and reserves human attention for the decisions that matter most.

And, as digital and phygital ecosystems broaden across suppliers, platforms and regulatory regimes, the model offers a structure that can flex without losing control.

Total Quality in practice



In consumer electronics

A Total Quality approach means treating the device, software and security as one system. Smart TVs, wearables and home devices all carry a mix of usability, security and performance expectations, interoperability standards and regulatory requirements.

A Total Quality model brings those together early. Firmware changes, platform updates and security hardening are assessed against the same view of readiness. Supply chain dependencies – from chipsets to protocol libraries – sit in the same workflow, so gaps in compliance or emerging requirements are visible before products enter final testing. This creates fewer late surprises and a clearer path to launch.

In energy and utilities

A Total Quality approach means aligning upgrade testing, quality engineering, operational technology (OT), security and regulatory compliance across the same lifecycle. Modern energy systems depend on software-driven infrastructure – everything from digital substations to dynamic pricing engines, EV charging networks and smart meters.

A Total Quality model brings performance, security and compliance together under one view of the lifecycle. Interoperability issues between meters, comms hubs and the metering data network are identified alongside cyber risks and load-performance behaviour, not afterwards. As smart energy services update continuously, integrated assurance gives providers a faster, more reliable way to adapt to regulatory change.

Next steps

Modern systems aren't slowing down, and assurance can't afford to stand still. The organisations that move fastest with confidence will be the ones that treat assurance as a connected discipline, not a collection of separate tasks. A single system of assurance offers a future-proof approach to delivery.

Get in touch

✉ | Email us at : **hello@resillion.com**

Or take a look at our website: **resillion.com/totalquality**

resill!on