Compliance Is Not Resilience

Compliance impresses regulators; resilience deters adversaries, and the coming decade will be won by the institutions that know the difference.

The Titanic complied with every maritime regulation in force when she sailed and carried more lifeboat capacity than the law required. The failure lay elsewhere: the regulations embodied assumptions inherited from an earlier age, and more than 1,500 people died within the protection of rules that events had overtaken.

For most of the post-Cold War era, Western institutions have operated on the same reassuring assumption: if a risk could be identified, documented, regulated and audited, it could be managed. Compliance became the organising discipline of modern governance. Governments built regulatory frameworks and corporations expanded their risk functions; boards accumulated policies, controls and assurance mechanisms. Across democratic societies, confidence grew that good governance could be demonstrated through documentation. That assumption is colliding with a more adversarial world.

The defining risks of this century are proving resistant to the systems designed to contain them. Cyber warfare, economic coercion, supply-chain disruption, disinformation, infrastructure sabotage, artificial intelligence competition and strategic dependency share one trait: each exploits the seams between established frameworks rather than operating within them. They move faster than

regulation adapts, while the most dangerous are deliberately engineered around conventional oversight.

Australia ran a live experiment earlier this year. When conflict disrupted shipping through the Strait of Hormuz, the country discovered the difference between being compliant and being resilient. Its fuel-security obligations had been satisfied, yet some reserves counted towards national holdings sat overseas under ticketing arrangements. Within weeks, parts of the country faced diesel shortages, fuel standards were relaxed by emergency instrument and the government bought expensive supplies on global spot markets. The response arrived in this year's budget: a $14.8 billion Fuel Security and Resilience Package, including Australia's first government-owned strategic fuel reserve and an increase in minimum onshore stockholdings from 21 days towards 50.

The lesson reaches far beyond energy policy. Modern institutions have become highly effective at proving compliance without necessarily proving resilience, and the distinction now carries strategic weight. Compliance asks whether an organisation conforms to established standards; resilience asks whether it continues functioning when those standards prove inadequate. In the stable decades after the Cold War the distinction could remain theoretical; in a contested system it is fundamental.

> "There is no reinsurance market for adversarial statecraft."

Consider how an adversary actually behaves. Economic coercion ignores regulatory boundaries, and hostile cyber actors operate beyond the perimeter that audit frameworks were designed to inspect. Foreign intelligence services are unconstrained by reporting standards or institutional definitions of risk; their objective is to exploit the assumptions embedded within the rules. That creates exposure conventional assurance struggles to price. No insurance policy can compensate a country for a telecommunications failure engineered by a hostile state, no compliance framework can prevent a coordinated campaign to corrupt an information environment, and no balance sheet captures the cost of discovering that a critical technology or supply chain depends on an adversary. There is no reinsurance market for adversarial statecraft.

Cryptography demonstrates the problem at its starkest. Security agencies warn that hostile actors are harvesting encrypted information today to decrypt once quantum computing matures, meaning commercial data, government records and intellectual property may already have been stolen even though their contents remain unreadable. The United States published its first post-quantum encryption standards in 2024 and urged immediate migration. For institutions holding information with long-term value, compromise can precede exploitation by years, and traditional assurance struggles with that chronology. No audit can reveal which archives an adversary has already collected or what they will be

worth in a decade, and attestation will not restore confidentiality once decryption arrives.

The most advanced regulators are beginning to recognise this limitation after decades in which supervision centred on documentation. Since March 2025, financial institutions in the United Kingdom have been required to demonstrate that important business services can continue through severe but plausible disruption, shifting the emphasis from proving a framework exists to demonstrating it works under pressure. The European Union has pushed further. Under the Digital Operational Resilience Act, applicable since January 2025, major financial institutions can be subjected to threat-led penetration testing with intelligence-informed red teams replicating sophisticated adversaries against live systems under supervisory oversight. The symbolism matters: a regulator that once requested policy documents now commissions people to attack the systems those policies supposedly protect. Demonstration is beginning to replace documentation as the unit of assurance.

What regulators demand of banks, states now demand of whole societies. Sweden distributed crisis-preparedness guidance to every household and this year reorganised its civil-contingencies agency into a Civil Defence and Resilience Agency, part of a wider European reassessment. NATO evaluates member states against seven baseline resilience requirements spanning continuity of government, communications, transport, energy, food and water in crisis. The governing question is changing from what a state has promised to what it can withstand.

This is the illusion of cover: the belief that documented compliance constitutes protection against undocumented threats, and its consequences run across entire economies. Financial systems can satisfy exacting regulatory requirements while depending on a handful of digital platforms and technological chokepoints; Australia's superannuation pool reached $4.8 trillion in June under intensive prudential supervision, yet exposure to opaque algorithmic market infrastructure fits uneasily within conventional regulatory returns. Economies can maintain exemplary governance while productive capability erodes; Harvard's Growth Lab ranks Australia 74th of 145 economiesfor complexity, second-lowest in the OECD. An institution can become steadily better governed against yesterday's risks while growing more vulnerable to tomorrow's.

Compliance earned its place: it professionalised the institutions of the democratic world, and orderly markets, public trust and accountability still rest on its foundations. It has ceased to be sufficient. Nor should resilience become compliance under another name: exercises grow predictable, testing turns performative and metrics become targets, until organisations optimise resilience scores as effectively as they once optimised compliance ones. Genuine resilience requires something harder to manufacture, evidence that systems continue functioning under conditions they were never designed to meet.

The direction of travel is clear: institutional credibility is migrating from what organisations can attest to what they can endure. Within a decade, demonstrated resilience could influence access to capital, insurance pricing, regulatory standing, sovereign creditworthiness and alliance relationships as profoundly as audited compliance shaped them over the previous generation.

The shift reaches into boardrooms and cabinets. Directors need to weigh the cost of inaction alongside the cost of action, and governments must treat strategic dependencies in energy, technology, data, communications and cryptography with the seriousness once reserved for national security. Critical services should be tested to failure rather than assessed for conformity, supply chains evaluated against coercion as well as efficiency, and data protected according to how long an adversary may value it. Here, open societies possess an advantage they rarely describe as strategic. Democracies can expose weaknesses, conduct public inquiries, acknowledge failure and rehearse crises before reality imposes them; authoritarian systems struggle because admitting vulnerability carries political risk. Resilience depends on material capability, and it rests just as heavily on the institutional willingness to discover uncomfortable truths before an adversary does.

The institutions of the coming decade will be judged as the Titanic was, on whether they continue to function when events outrun the systems that certified them. Compliance was the governing discipline of a stable world. Resilience will be the governing discipline of the contested one.